Psychological Defence Agency

JAMES PAMMENT, JESPER FALKHEIMER & ELSA ISAKSSON

Malign foreign interference and information influence on video game platforms: understanding the adversarial playbook

MPF REPORT SERIES 3/2023

MALIGN FOREIGN INTERFERENCE AND INFORMATION INFLUENCE ON VIDEO GAME PLATFORMS: UNDERSTANDING THE ADVERSARIAL PLAYBOOK

Photo: Pixabay

Print: Scandinavian Print Group AB

Production: Kid id

ISBN: 978–91–527–8768–7

Contents

Foreword

The controversy regarding the potential negative impact of video games on its users has come and gone in various guises ever since the first games entered the market. Today, gaming is a global billion-dollar entertainment industry with revenues outnumbering both the film and music industries. Given the rapid growth and widespread popularity around the world, its vulnerability for malign foreign interference and information influence should come as no surprise.

This study highlights how gaming platforms can be used by foreign powers for malign interference and information influence. The study takes a holistic approach outlining many of the problems, vulnerabilities, and challenges Western nations face ahead. The report builds on evidence from actual cases as well as the current literature in outlining the playing field. In view of the growing importance of this specific area within gaming, and its general lack of research, this study constitutes a timely contribution to Sweden's psychological defence both in terms of updated knowledge as well as suggestions for policy-relevant recommendations for further consideration.

It should be recognised that Sweden has an innovative and internationally renowned gaming industry producing titles played across the globe. We also have successful Swedish e-sports teams, these are parts of increasing influence in society that brings challenges as well as possibilities. It could well be argued that gamers as well as the gaming industry are served by more conscious eyes being open on gaming platforms – and call on players, developers, journalists, researchers, our international counterparts and other good forces to take an interest in the fact that video games are vulnerable to undue informational influence. I am encouraged that conditions for common ground can be found, and that further exploring of how gaming can be vulnerable to foreign influence – or be part of building resilience against it, will be a joint effort together with the gaming industry and not least gamers themselves.

Actors exploiting video games to spread malign foreign interference and information influence may want to see us Doomed. But as any modern space marine would do – the more skill points we assign into awareness and knowledge, the better chance we stand against them. This is the first report as part of the multi-year support the Swedish Psychological Defence Agency provides to the Psychological Defence Research Institute at Lund University.

The authors are responsible for the content and conclusions of this study.

Magnus Hjort
Director General

Swedish summary

Vi lever i en tid där omfattningen av otillbörlig kognitiv informationspåverkan från främmande makt med syfte att påverka människors uppfattningar, beteenden och beslut ökar. Särskild uppmärksamhet har riktats mot sociala mediers betydelse och potentiella effekter. Men det finns en stor digital sektor som hamnat utanför strålkastarljuset – dataspel inklusive de plattformar och sociala aktiviteter som är associerade med dessa (i rapporten benämnt som dataspelsdomänen). Enligt vissa källor spelar 82 % av internetanvändarna världen över dataspel (särskilt mobila), vilket motsvarar över 40 % av världens befolkning. Tilläggas bör att dataspel oftast är till stor glädje för dess användare. Forskningen om dataspel ger inte underlag för att dra generella slutsatser om direkta negativa effekter av spel. Men det finns studier som också påvisar negativa effekter (från beroende till radikalisering eller extremism) under vissa förutsättningar.

I denna rapport presenteras en kartläggning av dataspelsdomänen och en analys av hot och sårbarheter i relation till otillbörlig informationspåverkan såsom spridning av desinformation från främmande makter. I rapporten beskrivs och kategoriseras de hot och sårbarheter som dataspelsdomänen bär med sig. Beskrivningen bygger på kända fall av otillbörlig påverkan i eller genom dataspel eller spelangränsande plattformar, baserat på en genomgång av tillgänglig litteratur. I rapporten identifieras mer än 40 påverkanstekniker som framgångsrikt har riktat sig mot speldomänen och som i förlängningen skulle kunna användas för otillbörlig informationspåverkan av hotaktörer från främmande makter.

I rapporten berättas också om historien om kognitiv påverkan genom videospel (en forskningsöversikt om påverkan genom speldesign, sociala funktioner, social representation, opinionsbildning och i rekryteringssyfte) samt om dataspelsindustrin. Tidigare studier om dataspel och påverkan har i huvudsak genomförts med fokus på extremism, terrorism och hatretorik. I rapporten ges avslutningsvis en översikt över de viktigaste spelplattformarna och hur spelindustrin har hanterat olika kontroverser och policyfrågor.

Introduction

The power of video games to influence players is nothing new. Since the US congressional hearings of the early 1990s on video games and violence, the development of innovative new digital technologies has been accompanied by not-so-innovative fears about the damage video games might do to young and vulnerable minds. While research is largely inconclusive about direct correlations between gaming and problematic behaviours, there is still a widespread assumption that games can have significant effects, both good and bad. According to some, games can improve logical problem-solving, hand-to-eye coordination, and access to quality information; for others, they encourage anti-social behaviour, radicalise with extremist ideologies, and facilitate the sharing of classified, harmful, and hateful content. There is evidence to support both views.

One fundamental premise in this report is that games have persuasive, ideological and political dimensions. As argued by Foust (2021), video games are not politically neutral, apolitical spaces where people simply interact and play cooperatively. Rather, they are "… vibrant, contested, growing, lucrative, politicised spaces, where actors of all sizes and ideologies compete to influence the minds of their audiences. Video games are where politics happen". Games are appealing tools for strategic communication and propaganda because they provide a relatively inexpensive way to reach audiences and monitor audience reactions (Schulzke, 2013). According to some sources, 82% of internet users globally play video games, equating to over 40% of the world's population[1]. It is surprising then that this major social, cultural, economic, and political industry has not been considered alongside other digital media, and particularly social media, as a core component of public deliberation and human interaction in the digital age. As part of the Lund University Psychological Defence Research Institute's research track of exploring the potential for malign foreign influence in unknown, under-researched spaces, this report seeks to take significant steps in improving knowledge of the video games sector.

Most studies of malign information influence focus on social and traditional media; both the threats that target them, and the vulnerabilities inherent in their usage. Following Russian interference in the 2016 US Presidential Election, it has been a priority for many democratic governments to better understand how vulnerabilities in their information ecosystems are exploited by threat actors, whether those threat actors be hostile states, organised criminals, or extremist groups. The domain of video games – broadly consisting of the industry, gaming platforms, game-adjacent social platforms,the games themselves, and the players – appears to have been largely neglected in these analyses. This report explores the available evidence to assess the vulnerabilities that the video game domain possesses. All evidence is derived from actual known cases of malign influence within video games or game-adjacent platforms, based on a review of available literature together with an in-depth threat and vulnerabilities assessment.

Chapter 1 serves as an executive summary of the findings of the report as a whole. It outlines the playbook that threat actors are likely to draw from if they conduct foreign interference and information influence targeting the

[1] https://www.bankmycell.com/blog/how-many-people-play-video-games

gaming domain. It begins with a short introduction to foreign interference and information influence. Subsequently, a threat and vulnerability assessment outlines the main influence techniques and vulnerabilities available to threat actors who might target gaming. Following that, a brief assessment is made of specific threat scenarios, with a focus on coordinated influence campaigns. The section ends with a policy briefing and recommendations.

Chapter 2 of the report tells the story of how cognitive influence has been understood in the context of video games, such as longstanding fears about violence and addiction. It describes the basics of the video games industry and offers an overview of research about influence through game design, social functions, social representation, advocacy, and for the purposes of recruitment. This includes the benign and positive cognitive effects of video games as those effects are currently understood by researchers.

Chapter 3 reviews current research about how games and game-adjacent platforms have been used for malign influence. This mostly empirical discussion focuses on a wide range of exploits that provide the procedural and detailed evidence supporting the results outlined in Chapter 1. Many of the examples come from the two main approaches researchers have used to analyse exploitation of video games in contemporary research: extremism/terrorism (both Islamic and far right) and hate speech. The techniques themselves are however actor agnostic and could be used by anyone with the appropriate motivation and resources.

Chapter 4 offers a brief overview of the main gaming platforms and some of the controversies and policy issues that have shaped their relationship to discussions of malign information influence and interference through gaming. The aim of this section is to help to develop more platform-specific knowledge of the current state of the gaming field.

In our view, it is possible to identify in excess of 40 influence techniques that have successfully targeted the gaming domain and that could, by extension, be used by threat actors to achieve objectives related to malign influence and foreign interference. It is also our view that, in comparison to the social media sector, **the gaming domain is ripe with vulnerabilities and has insufficient policies and mechanisms to cope with motivated information influence campaigns.** Nor are there sufficient avenues for researchers, journalists, and arguably the industry itself to better understand the degree to which gaming platforms are currently being exploited by threat actors. **In other words, not only do we not know how serious the situation presently is, we also lack the means to find out.**

Since the 2016 US Presidential Election and the subsequent Cambridge Analytica scandal and Mueller investigation into Russian election interference, social media has been forced to recognise its vulnerabilities in relation to the illicit activities of motivated threat actors. In our view, **the video game domain is ripe for scandals of a similar scale and impact to 2016.** Whether it will end up being the result of a systems breach, a multifaceted influence operation, a data privacy revelation, or a money laundering scandal, video games are overdue their 2016 moment. **The question is, how prepared will the industry, governments, and gamers be to deal with it?**

1| Threat and vulnerability assessment

1. Threat and vulnerability assessment

The video game industry is still traumatised by the video game violence debates and congressional hearings of the 1990s. But these may be nothing compared to the controversies to come. It is the conclusion of this report that the spread of top-secret intelligence on Discord[2] , the creation of games and mods that gamify real-world atrocities, and radicalisation within tight-knit online communities, are the tip of the iceberg. As mentioned earlier, the industry has steered clear of a Cambridge Analytica-type scandal about user privacy and misuse of personal data for psychographic targeting, and there has yet to be a case of coordinated exploitation of gaming and game-adjacent platforms akin to Russian interference in the 2016 US Presidential Election. Yet with a potential market of over 3 billion video game players globally, the stakes are high.

To what extent are such scenarios plausible? This chapter provides an assessment of the risks and vulnerabilities of foreign interference and information influence on gaming and game adjacent platforms. Drawing upon insights from decades of research into video games covered in subsequent chapters, it identifies known exploits and vulnerabilities in the industry and considers how such techniques might be adopted by threat actors seeking to expand their options for malign influence. In other words, almost everything mentioned in this chapter has already happened, just not necessarily for the purposes of foreign interference and information influence. The chapter identifies over 40 significant influence techniques that would reasonably be expected to be part of the playbook threat actors engaged in foreign interference and information influence would draw upon. While any individual technique may be used by a threat actor, coordinated efforts that combine multiple techniques into a concerted influence campaign provide a significantly higher threat. The chapter outlines some scenarios in which coordination would enhance the level of threat.

This chapter is designed to provide an introductory resource to researchers and analysts whose task is to better understand where to focus their resources. Assessing to what extent hostile foreign interference and information influence are taking place on gaming and game adjacent platforms is a gargantuan task, not least because it is characterised by unknown unknowns. Analysts will find this chapter most useful for an overview of the field's threat actors, vulnerabilities, risks, and policies. The systematic breakdown of tactics and techniques is the first of its kind. Researchers will perhaps find in this chapter

[2]The Pentagon Leaks 2023 on Discord, see: https://www.theguardian.com/us-news/pentagon-leaks

some support regarding which areas of the issue to focus upon, although Chapters 2 – 3, which represent one of the first major literature reviews of research pertaining to information influence in video games, might provide more useful direction.

Foreign interference & information influence

Information influence is a form of cognitive influence conducted by foreign powers, or their agents, to influence the perceptions, behaviour, and decisions of target groups to the benefit of those foreign powers. It can be conducted as a single activity or as part of a larger operation combining multiple activities. Increasingly, these activities are interpreted in the context of the coordinated efforts of a foreign power to exert illegitimate influence, where each activity (or operation) has one or several ends of their own intended to help achieve a more significant goal. This could include influencing (1) the decisions of politicians and other decision-makers in the public sector; (2) parts or the whole of public opinion; (3) political decisions or public opinion in other countries where sovereignty, the goals of security, or other national interests can be negatively affected (Pamment, et al., 2018). It is therefore increasingly common to refer to foreign information manipulation and interference, since the information influence activities are often indistinguishable from a wider effort of a threat actor to interfere in targeted countries (European Union External Action Service, 2023).

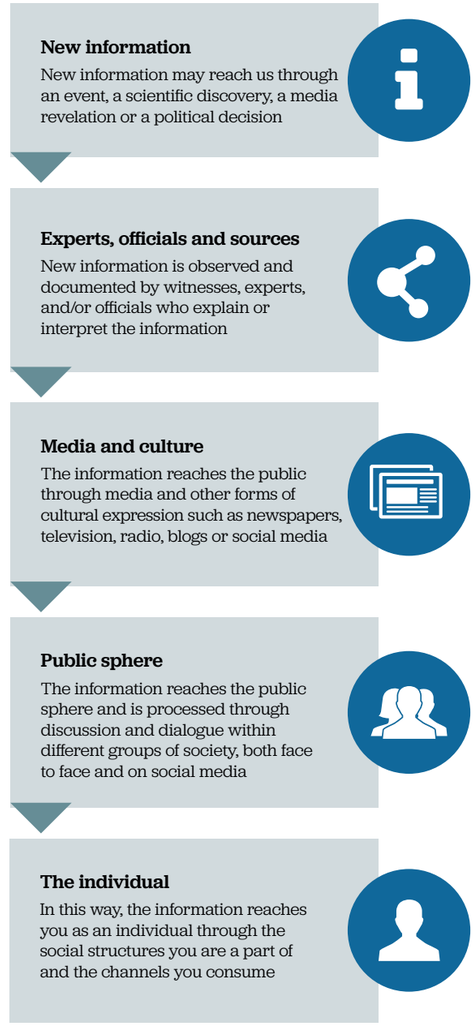
Many studies of information influence focus on social and traditional media, and particularly the interplay between the two. Following 2016's Cambridge Analytica scandal and the associated Russian interference in the US Presidential Election, it has been a priority for many democratic governments to better understand how vulnerabilities in their information ecosystems are exploited by threat actors, whether they be for example hostile states, organised criminals, or extremist groups. One digital media domain appears to have been largely neglected in these analyses, however. That domain is video games, understood in the broadest sense including the platforms and social activities adjacent to the games themselves. This report explores the available evidence to assess the vulnerabilities that the video game domain possesses. All evidence is derived from actual known cases of illegitimate influence within video games or game-adjacent platforms.

Influence is by its nature intangible. That means that it is often challenging to identify and prove the extent to which someone was influenced. Instead, assessments of this kind often focus on risk and vulnerabilities, and in particular the risks posed by certain types of threat actors (e.g., countries, organisations, individuals) and the vulnerabilities in a domain (e.g., video games and game-adjacent platforms). This means that the assessment is often speculative, especially when it is not focused on a specific case. It is not the purpose of this report to state categorically that Country A is conducting influence operations targeting video game audiences in Country B. Rather, the goal is to assess risk and vulnerabilities by establishing an evidence base and a framework for analysis. This will enable improved decision-making and preparedness in this domain by governments, the video games industry, and video gamers. In previous research on information influence, we have attempted to

explain how malign foreign influence takes place with a simple model (Swedish Civil Contingencies Agency, 2018). For this model to work, we need to assume that opinions are formed as a result of a reasonably rational process that begins with something happening or new information coming to light. Witnesses, scientists, officials, and other individuals with credibility in an area confirm, interpret, and/or explain the situation. The media pick up the information together with interviews with credible sources and spread it through their channels. This information will then reach different groups in society through whichever channels they rely upon, which includes via friends and family, both online and real-world. Of course, opinion formation does not always work like this in practice, but this is broadly how the process of opinion formation in a democratic society is supposed to work in theory (Nothhaft et al 2018).

This process is based on a few basic principles. First, it depends on the event or information being correct and based on facts, i.e., that somebody isn't just making something up or is engaging in deliberate subterfuge. It also assumes that the claim is verified by credible sources in the form of individuals whose reputation will be undermined if they lie or misinform. It assumes that the media that pick up the story are balanced in their coverage, that they double-check facts and sources, and that they strive to serve the public interest. One might also expect discussions across various groups of society to take differing voices and opinions into account and hold a balanced and constructive debate before drawing conclusions.

Information influence activities exploit situations in which opinion forming deviates from the process described above. Through opportunistic (or systematic), creative (or predictable), and technologically advanced (or, indeed, very basic) methods, foreign powers can direct their influence techniques at vulnerabilities in the opinion-forming process in order to compromise the flow of information. One should assume in this case that threat



actors are focused upon identifying vulnerabilities in how critical information travels through the media landscape and in how our brains process information, for the purpose of manipulation.

Facts can be falsified or manipulated. False experts can be called in, and witnesses can be coerced. News services can be run as one-sided propaganda channels, and the digital public discourse can be conducted between automated bots that create the false appearance of a lively public debate. When these activities are carried out deliberately, sometimes in the form of coordinated campaigns with the aim of undermining democratic processes, we cannot always rely on the democratic process of opinion formation to self-correct (Nothhaft et al 2018).

In video games and game-adjacent platforms, we observe different methods of malign influence to those used in traditional and social media. However, the goal of gaining influence over perceptions of reality follows similar principles. For example, new information can circulate within games (e.g. altered historical details) or on game-adjacent platforms (e.g. disinformation spread through chat). Experts and sources might be influencers who have tremendous respect within their gaming communities, but whose allegiances can be bought or have an ideological agenda. Media and culture include cultural artefacts (e.g. video games and game aesthetics) as well as niche news sources that might make false claims about e.g. a military attack using realistic video game footage. The public sphere in gaming is active and largely unmoderated, providing multiple channels of direct influence between players whose identities are obscured behind usernames and avatars. And the individual has cognitive biases that have for decades been explored in the context of gaming (e.g. violence and addiction). In sum, many of the same vulnerabilities associated with social and digital media apply to video games. This chapter outlines which, and to what extent we should be concerned about them from a malign interference and interference perspective.

Threat assessment

This report represents an effort to collect knowledge about how foreign information influence and interference can take place through video games and game-adjacent platforms. While it explores the nature of the threat, it does not make use of intelligence about which actors provide the highest threat. As such, the threat assessment presented here is limited to outlining characteristics of the types of actors who may be expected to have an interest in exploiting vulnerabilities in this domain.

This threat assessment is divided into three sections. The first two sections cover types of actors: state actors and non-state actors. The analysis of each is subdivided into three parts: an outline of capabilities (i.e., the relevant skills and means at the actor's disposal); a suggestion of intent (i.e., the likely motivations an actor might have to carry out these activities); and an overview of resources (i.e., the assets an actor would be expected to control and draw upon). Together, this helps to paint a picture of the types of threat actors who may be drawn to conducting influence operations on video games and game-adjacent platforms.

The third section of the threat assessment covers the key areas of video gaming that may be under threat. These represent aspects of the gaming domain which can be targeted individually or in coordination to create an influence effect. In other words, they are areas of vulnerability, the details of which are investigated more fully in the following sections. Subsequent chapters of this report spell out many of the tactics, techniques, and procedures (TTPs) that have been used by threat actors to target the gaming domain over the past two decades.

State threats

State actors refer to the formal structures that act on behalf of a government, including management of a country's political, economic, diplomatic, military, and informational domains. States with an interest in pursuing information influence in the video game sector are likely to possess the following characteristics:

Capabilities

- A track record of using their cyber, hybrid, influence, and intelligence capabilities for offensive purposes
- Cultural production and power projection capabilities including in the video game sector
- Holistic situational awareness for example through the ability to merge open and classified datasets and data sources

Intent

- An interest in projecting national identity, cultural identity, and/or power
- Authoritarian regime with an interest in censorship, repression & restriction
- An existing interest in information influence and interference on social and other digital media
- A track record of exfiltrating IP, personal data, and other sensitive information

Resources

- Soft and sharp power assets
- A national gaming industry, and/or international purchases of gaming studios
- Access to non-state threat actors with advanced capabilities (below)
- Access to exfiltrated information and/or data
- Access to government datasets, including intelligence
- Diaspora and extended international network, national and cultural loyalty/affiliation
- Foreign agents

Non-state threats

Non-state actors are organisations without official affiliation with governments, though in many cases formal or informal relationships exist. Nonstate actors with an interest in pursuing information influence in the video game sector are likely to possess the following characteristics:

Capabilities

- Propaganda and information influence production, especially digital content and digital relationships
- Cyber capabilities, including phishing and hacking
- Audience insight, especially through cultural affiliation
- Open-source intelligence (OSINT)

Intent

- Terrorism & extremism
- Activism, advocacy & political
- Commercial (influence for hire)
- Criminal
- Hacking
- Motivated individuals

Resources

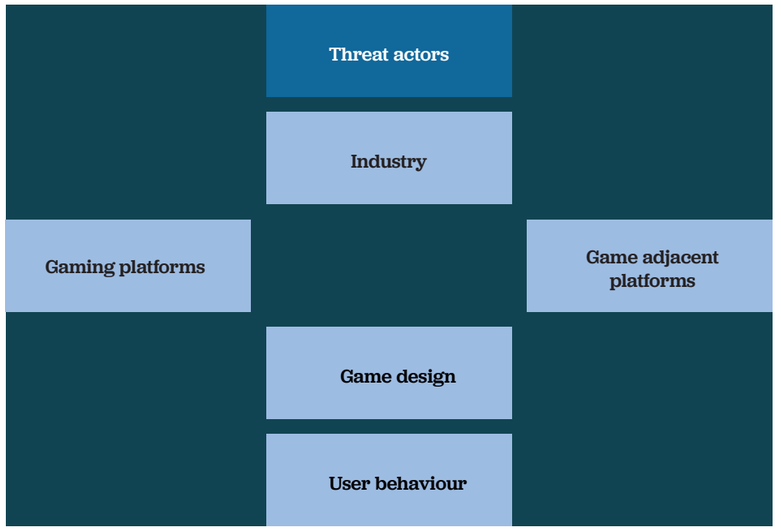
- Loyalty built up over time with gaming communities
- Loyalty created through ideology, sense of purpose, and understanding of grievances
- International support networks of likeminded organisations
- International support networks of likeminded individuals
- Ability to draw on governmental networks, including intelligence sources
- Access to exfiltrated information and/or data

Key areas for exploitation

Illustrated on the next page are some of the key areas that a threat actor is likely to seek to exploit. These five areas are referred to throughout this chapter, most importantly with regard to how tactics are designed to create influence effects. They overlap to a certain degree, and in many cases a threat actor will work through one of the areas to create an influence effect in another.

- *The gaming industry.* E.g. companies, owners, industry associations, executives, studios, coders, influencers.
- *Gaming platforms.* E.g. subscriptions, online services, payment services, pre-paid payment cards, algorithms, advertising.
- *Game-adjacent platforms.* E.g. communities, algorithms, chat, forums, social media functions, audio-visual-textual sharing functions, advertising.
- *Game design.* E.g. narratives, aesthetics, characters, mechanics, in-game currency, mods, cheats, AI, VR, AR.
- *User behaviour.* E.g. cognition, gaming and game adjacent activities, purchasing behaviour, cross-platform behaviour, data privacy behaviour.

Key areas for exploitation



These areas are broad, and they are not all under the control of a single actor. Rather, they may be considered the key areas in which threat actors seek out vulnerabilities. The following sections of this chapter will demonstrate, through six specific tactics subdivided into over 40 influence techniques, how vulnerabilities within – and between – these areas can be exploited. Once again, all examples referred to in this analysis have been used by threat actors in the video game sector previously, just not necessarily for the purposes of foreign information manipulation and interference.

Tactics, techniques & procedures

Tactics, techniques, and procedures, or TTPs for short, refer to the way in which information influence and interference measures can be codified so that different analysts understand the activities in similar ways. TTPs are used extensively in the cybersecurity world and to a lesser extent in analysing information influence. In the latter case, the standards are still emerging. While we take inspiration from e.g. the DISARM Framework, for the purposes of this analysis we have outlined a distinct set of TTPs based on the specific demands of the video game domain. They are a starting point for more detailed analysis.

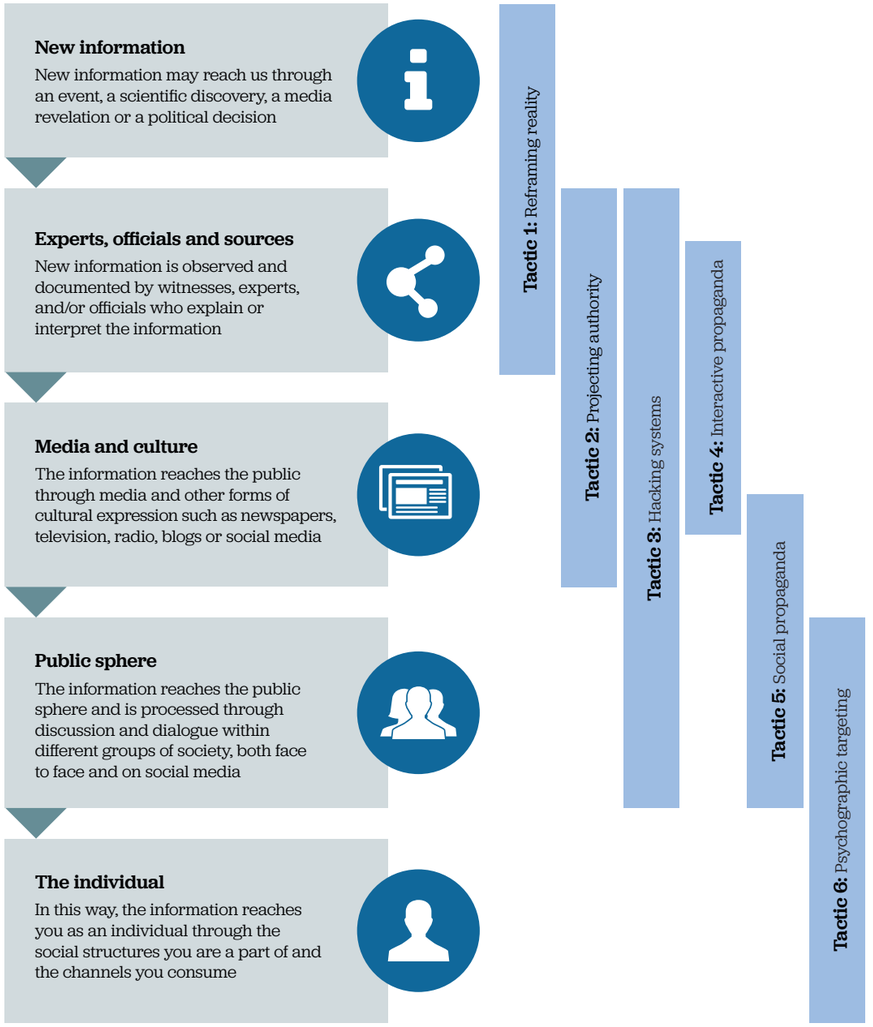
According to the National Institute of Standards and Technology (NIST), the US body which manages many of the international standards for cybersecurity, TTPs refer broadly to the behaviour of a threat actor as it is observed through their actions[3]

- A tactic is the highest-level description of the behaviour, covering how an anticipated goal is to be achieved; for example, a tactic may be to attempt to spread disinformation about a battle.
- Techniques provide a more detailed description of the behaviour, covering activities that support the tactic; for example, a news report may deliberately use realistic video game footage to spread disinformation about a battle to a public who receives most of their news through television.
- Procedures provide a lower-level, highly detailed description of the behaviour in the context of a technique; e.g., a detailed description of how certain graphical settings, mods, and data capture methods were used to create fake footage and how it was shared through social functions before reaching the news media.

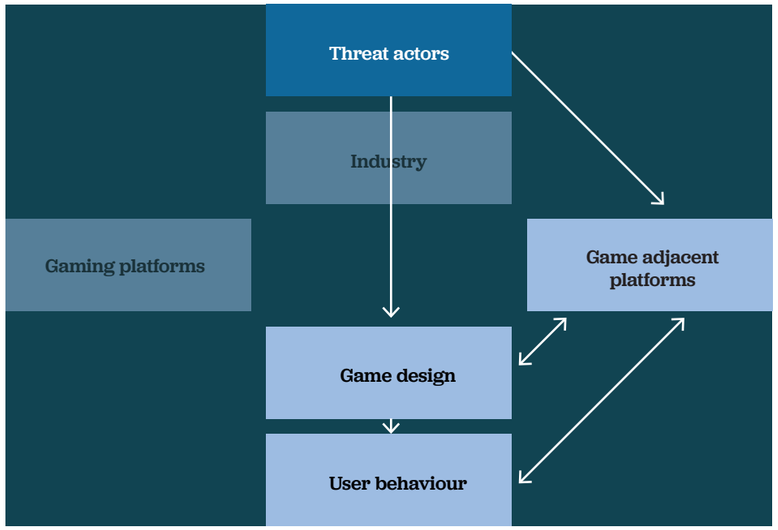
This list of TTPs was derived from two data collection exercises that were conducted specifically for the purpose of preparing this report. The first is a broad literature review of relevant research that is summarised in parts 2–4 of the report. The second is a number of meetings and workshops with experts in gaming, including researchers, industry representatives, and government representatives. Based on this analysis, we identified over 40 individual influence techniques that could be grouped into 6 overall tactics.

The focus here is on tactics and techniques. Examples of procedures, that is to say, more detailed and contextual information about individual techniques, is given throughout the evidence in chapters 2–4 of the report. Procedures in this sense represent the detailed descriptions of specific activities that may be seen as contributing to the achievement of tactics and techniques. The 6 tactics are as follows:

[3] https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures



Reframing reality



Tactic 1

Video game content is used to reframe perceptions and interpretations of reality; for example to

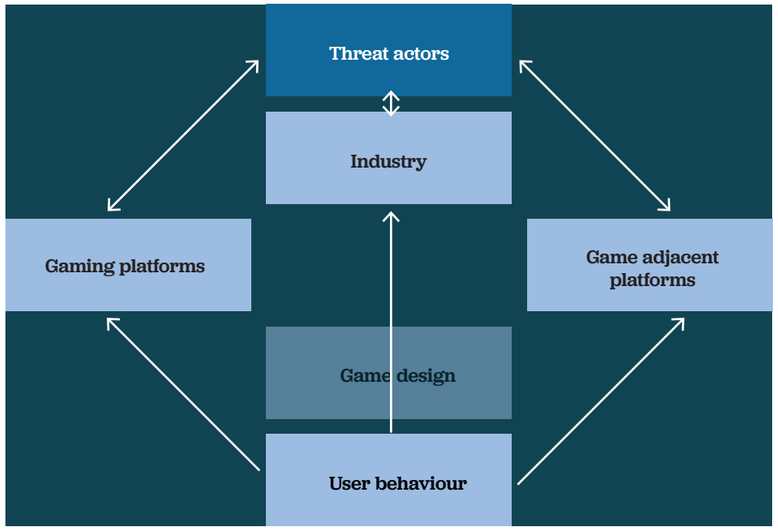
- Dispute history, change facts or disinform about real-life situations
- Adopt gaming tropes in real-life situations
- Dehumanise through gamification of real-life situations

Threat actors use this tactic when they seek to leverage aspects of video games – including their aesthetics, storytelling, game mechanics, and realism – to their advantage. They target primarily the social functions of game-adjacent platforms and use a shared interest in video games to create a common language of imagery, symbols, and rhetoric. This can be employed to the blur distinctions between games and reality; for example, by using footage from games to 'stand-in' for real-world events, gamifying real-world activities including violence, and adopting video game tropes in propaganda.

Techniques

- Video game content is purposefully or accidently used to represent a current affairs event
- Naturalistic games purposefully or accidently change or misrepresent key historical or representational details
- Propaganda content or ideology in video games is consciously adopted by real-world communities
- Video game imagery and gamified language is purposefully mimicked or referenced in real-world situations
- Video game mechanics are used to train tactics so that they can be applied to real-life situations
- Video game mechanics are used to justify, intensify, or otherwise gamify harmful real-life situations
- AR tools are used to guide or gamify real-world actions

Projecting authority



Tactic 2

Video games are used to assert authority in order to further geopolitical or political-economic competition; for example to

- Censor and encourage self-censorship in line with authoritarian norms and values
- Harvest data
- Conduct espionage

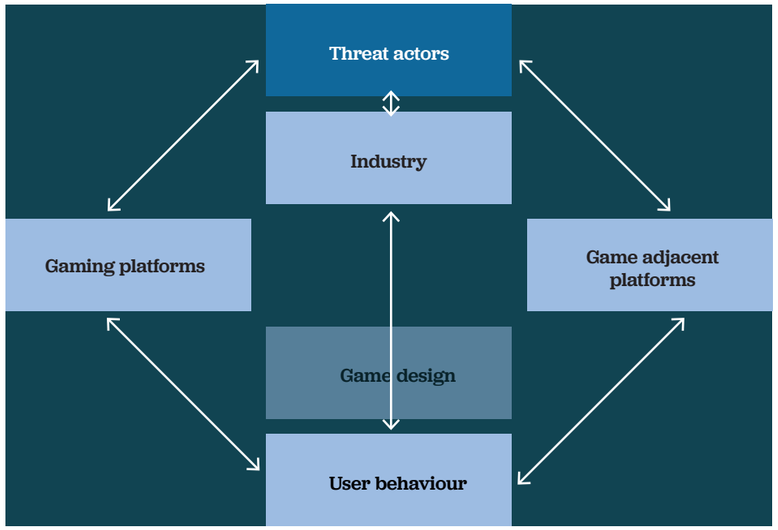
Tactic 2 involves threat actors using video games to directly further their objectives in cultural, political, economic, or geopolitical competition. This sees the gaming industry targeted as a sphere of influence or hybrid domain. Through direct ownership or indirect control over the gaming industry, threat actors seek to assert influence over the production of games as well as activities on game-adjacent platforms. This creates opportunities for cultural projection, censorship, surveillance, and data exfiltration.

Techniques

- Ownership of gaming studios by authoritarian states or organisations encourages the production of games promoting specific ideologies or censoring democratic norms and values
- Video game producers self-censor due to fear of exclusion from authoritarian markets
- 'Shovelware'[4] games are used to distribute a large amount of content on a specific theme or from a specific country, for the purpose of spreading propaganda, collecting data, or building a user base
- Opaque ownership of gaming studios enables surreptitious surveillance and collection of data or intelligence
- Video game tag names or avatars are used to mask the identity of foreign agents, extremists, or other harmful actors creating relationships and/or collecting intelligence on players
- AR games are used as cover for espionage

[4] Usually games of poor quality produced in large numbers, increasingly produced with the help of AI.

Hacking systems



Tactic 3

Video game & game adjacent data used to gain access or leverage over computer systems; for example for

- Hacking and phishing
- Gaining access to data in order to blackmail industry, individuals, and organisations
- Exploiting systems & mechanics connected to gaming

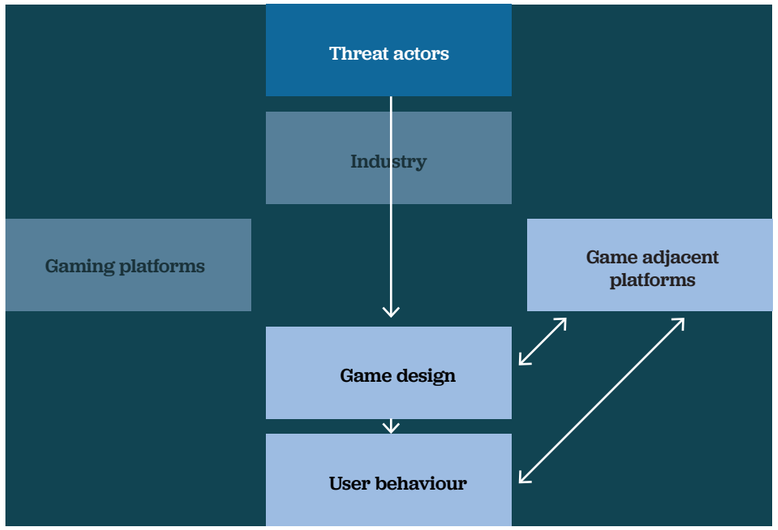
This tactic refers to when threat actors use cyber capabilities to gain access to systems belonging to gamers, organisations, as well as the gaming industry. Targets include all aspects of the gaming ecosystem, since all can potentially be exploited to enable access to systems. Hacks can for example begin with phishing efforts that mimic gaming platforms and especially currencies associated with them. Mods and pirated games also provide a vulnerability. Once a system has been hacked, a range of exploits are available in order to further the threat actor's objectives.

Other forms of control over video game systems include mechanics for creating value, such as scoreboards, in-game currencies, and pre-paid game vouchers.

Techniques

- Video games and adjacent services are used as threat vectors for phishing
- Video games and adjacent services are used to recruit and train users to act in a coordinated manner, for example, to manipulate, hack or 'game' services
- Code used to circumvent DRM or anti-cheat contains viruses, malware, or other backdoor exploits
- Hacking of individual or organisations' systems to gain control for botnets, DDOS attacks, crypto farming, passwords, and access to other personal data
- Hacking of video game companies or services for exfiltration of player data and/or proprietary industry data
- Control over stolen or hacked accounts/information owned by governments, companies, public services, and individuals is used for money laundering, blackmail or extortion
- Classified information and other harmful or illegal content is leaked through unmoderated gaming forums
- Economies within or adjacent to video games are used to launder money
- Pre-purchased game cards or vouchers are used to pay for restricted services or launder money

Interactive propaganda



Tactic 4

Video game design is used to promote interactive forms of propaganda; for example to:

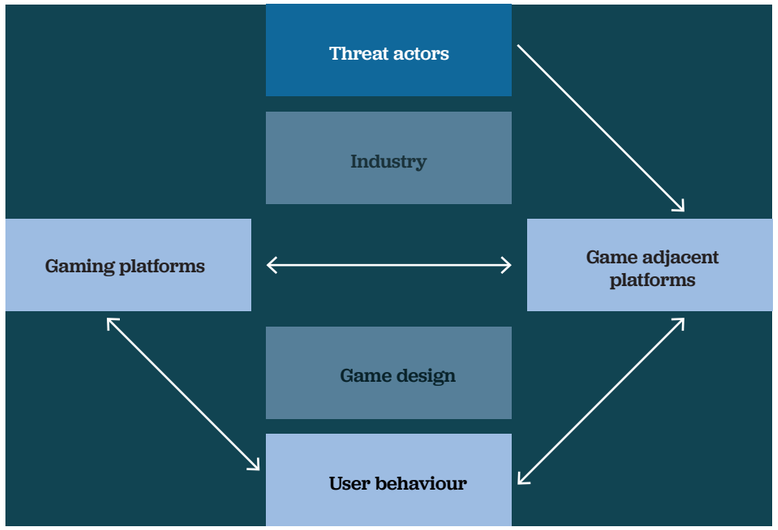
- Spread both traditional and interactive propaganda through games
- Establish relationships with players by forming in-game communities
- Radicalise & mobilise players

Tactic 4 encompasses the efforts by threat actors to create interactive experiences that are implicitly or explicitly in support of propaganda or ideological goals. They target primarily video games and can for example produce their own games often mimicking established franchises, create mods for existing games which grants easy access to an established audience, or purchase in-game advertising.

Techniques

- Propaganda content or ideology is placed in a video game narrative or game worl
- Propaganda content or ideology is promoted through advertisements in a video game narrative or game worl
- Mods are used to change the mechanics, aesthetics and themes of an established video game with propaganda supporting malign groups or interests
- Video game content allows targeting of and hate directed toward specific individuals, groups or interests in order to generate feelings of shared identity and empowerment
- Video game content allows targeting of and hate directed toward specific individuals, groups or interests in order to radicalise and/or mobilis
- Multiplayer video games used for bonding by malign communities seeking to exploit those relationships at a later date

Social propaganda



Tactic 5

Video game-adjacent platforms are used for propaganda through social connections; for example to

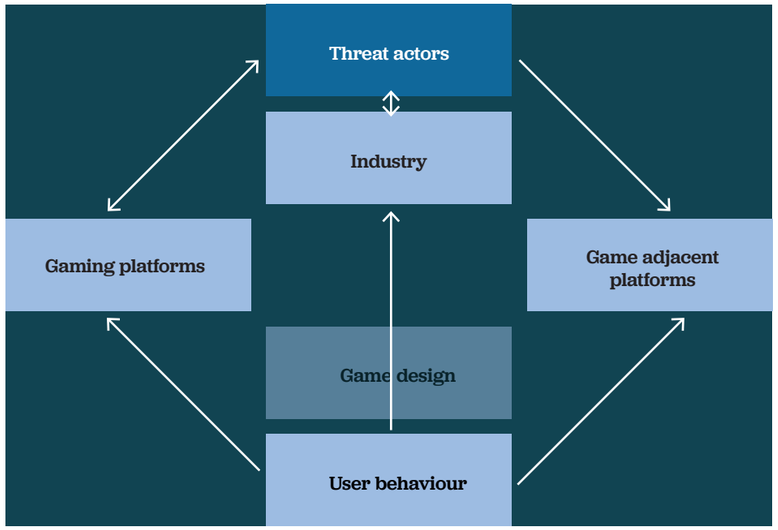
- Shape shared cultures with gaming as a common thread
- Use social functions to introduce propaganda and increase polarisation & intolerance
- Take advantage of gaps in content moderation & oversight to promote propaganda

Threat actors use Tactic 5 to shape communities in which their ideologies and propaganda can find fertile ground. Drawing on techniques that are broadly consistent with those used on social media, game-adjacent platforms provide a vector for threat actors to build relationships, spread propaganda, and heighten polarisation. The aim is often to create community bonds that carry over into different environments, including across and between tech platforms, or into real-life.

Techniques

- Video game adjacent communication functions such as chat used to spread propaganda
- False accounts are created to astroturf game-adjacent functions
- Video game adjacent communication functions such as chat used for harassment of groups or individuals
- Video game adjacent communication functions such as chat used to spread illegal content or links to harmful websites
- Propaganda content or ideology is promoted through advertisements on game adjacent platforms
- Tribal and polarised identities and behaviour associated with video games or video game platforms are channelled into non-gaming contexts
- Content moderation reporting functions are misused to temporarily ban or restrict user access to accounts
- Activities target known areas where platform terms of service are not fully enforced

Psychographic targeting



Tactic 6

Video game data is used for psychographic targeting and other forms of profiling; for example to

- Improve profiling and targeting of individual users or user segments
- Develop complex datasets
- Improve advertising

This tactic can be used by threat actors who wish to better know and understand individuals, groups, and market segments. Harvested data can be used to many ends. Profiling is most often used to improve the targeting of advertisements, though video game data identifying personality traits could also be used to support political-economic goals by for example identifying groups susceptible to certain messaging, supporting espionage, or using datasets to improve machine learning and AI.

Techniques

- Basic user data such as email addresses are harvested and sold
- Data collected from purchases, addictive gaming models, game-based decisions, and social interactions are used for psychographic targeting
- Data collected through cookies, trackers, microphones, and cameras are used to undermine user privacy
- Data collected from VR and AR are used to generate psychographic and physiological data profiles of individuals
- Data collected from video games are merged with other datasets such as social media to target users for political-economic purposes, enhance predictive AI, or advertising

Threat scenarios

The above TTPs provide a general overview of what analysts and researchers of foreign information manipulation and interference should look out for in the video game sector. More details of how this plays out in practice can be found in subsequent chapters. An important point to take into consideration at this stage, however, is that individual TTPs are rarely used in isolation. A threat actor seeking to achieve a specific influence goal using video games as a medium is likely to plan these activities as campaign; that is to say, as an influence operation consisting of several coordinated and synchronised parts. Since we lack a strong evidence base of concrete examples, we will instead highlight some scenarios which, based on prior knowledge of how influence operations are conducted in other domains, would be relevant to consider in the case of video games. These outlines of threat scenarios can also be used by analysts for risk assessment, capability assessment, red-teaming, and running tabletop exercises.

Elections scenario

In the weeks leading up to a general election, the major social media companies decide to restrict both political advertising and sharing of political links on their platforms. This is due to cuts in content moderation capabilities, a lack of local adaptation, as well as the risks of heavy fines for breaking political advertising regulations. Subsequently, hundreds of millions of dollars of advertising and advocacy efforts are instead directed to game-adjacent platforms. This includes:

- *Paid influencers:* Payments to video game influencers to integrate political messaging into their content.
- *Astroturfing:* Astroturfing efforts on game-adjacent platforms, e.g. through the coordinated creation of thousands of politically-engaged accounts.
- *Mods:* Creation of political mods for popular games that are used to create video assets and advertising.
- *Encouraging tribalism:* Establishment of polarised political teams playing games competitively, with the goal of eroding the political middle ground.
- *Money laundering:* Coordinated funnelling of funding to political parties through pre-purchased video game currencies and leveraging game currencies.

Recruitment scenario

An extremist group seeks to build relationships with a certain profile of gamer in support of a series of real-world political actions that involve harassment and violence. The group is targeting gamers and individuals who frequent gaming forums and communities to recruit new members and spread their message, first by forming what appears to be innocent friendships based on shared interests and shared grievances. The group uses several tactics to achieve this goal, including:

- *In-game chat functions:* Chat and messaging systems used to persuade, and eventually send propaganda, directly to players within the same game.
- *Game modifications:* The group creates mods that emphasise their message, for example by normalising violence against a specific group. These mods are shared through gaming forums and pirating websites.
- *Game-adjacent platforms:* The group utilises game-adjacent platforms to spread their propaganda message. By targeting these platforms, the group is able to reach a wider audience of gamers who may not necessarily be playing the same types of games. Some users may not even be players at all but rather interested in the community within these platforms.
- *Astroturfing:* Use of astroturfing tactics to create the illusion of widespread support for their cause. This includes the creation of sock puppet accounts and manipulated social engagements.
- *Video game footage in propaganda videos:* The group uses gameplay footage as a means of showing and gamifying their intended goals. Users are incentivised to mimic this footage in real life.
- *The use of game-play elements:* The group is incorporating game-play elements, such as achievements and rewards, into their propaganda message to shape audience behaviour, increase engagement, and encourage players to further spread their message.

War propaganda scenario

During an unpopular invasion by an authoritarian country against its neighbour, game-adjacent platforms are targeted as a means of spreading propaganda, controlling domestic dissent, and discrediting both the enemy and sources that provide facts about the conduct of the invasion. This includes:

- *Mods:* The authoritarian country creates and distributes pro-war mods that depict the invading army as heroes and the enemy as villains. These mods are shared through gaming forums and other online communities, creating a false narrative that supports the invasion.
- *Disinformation on game-adjacent platforms:* The seeding of disinformation messages on game-adjacent platforms as part of a campaign aiming to discredit the enemy and to provide a false justification for the invasion.
- *Promoting military recruitment through in-game advertising:* Use of in-game advertising to spread propaganda to players while they play.
- *Discrediting sources of information:* Use of game-adjacent platforms to discredit, harass and threaten sources that provide factual information about the conduct of the invasion.
- *Use of video game footage to create a false narrative:* Manipulation of video game footage to make it appear as if the enemy country is committing atrocities or war crimes, thus painting the enemy in negative light, and further justifying the invasion.
- *Controlling domestic dissent:* Using in-game messaging systems to monitor and censor messages that are critical of the invasion. Creation of fake accounts to engage in discussions on gaming forums, spreading disinformation, and attacking individuals who oppose the invasion.
- *Encouraging violence:* Use of mods, spread of videos, or messaging behaviour that normalises genocide and other atrocities against the enemy population.

Call to violence scenario

A threat actor disguises their identity and creates a Live Action Role-Playing Game (LARP) that intersects with video games. The "truth" of the mystery is hidden in game mods that must be decoded through following clues found both in the real-world, on websites, and in game-altering files, leading users to solve a conspiracy that promises real-world political implications.

- *Data collection:* Mods and AR enable data collection on LARP players as they work through the mystery.
- *Astroturfing:* Game-adjacent platforms used to create the impression of a large audience heavily invested in the LARP.
- *Narrative development:* Storytelling throughout the mystery normalises specific political standpoints that are conspiratorial in nature.
- *Multi-modal engagement:* Engagement through chat, forums, mods, and real-world activities creates a holistic sense of community and strong bonds between players.
- *Call to action:* Ultimately, these activities are used to support a call to action which is political in nature and could for example draw people into a demonstration at which threat actors are present and intend to cause violence on a specific group.

Repression scenario

An authoritarian country invests heavily both in domestic games production and in the purchasing of small, established game studios in democratic countries. The country aims to use the gaming industry to help spread its ideology and control the narrative both domestically and internationally. The tactics used by the authoritarian country include:

- *Purchasing small game studios:* Use of financial resources to influence the content produced by Western studios.
- *Setting up domestic gaming production:* Heavy investment in the domestic gaming industry to create a national gaming culture that aligns with its political ideology. This allows control of the narrative within their borders and to potentially export this ideology through globally popular games.
- *Creating game-adjunct platforms:* Creation of state-controlled gaming platforms that are heavily monitored.
- *Censorship and intimidation:* Use of censorship, bans, fines, threats, and intimidation against game studios and individuals who do not align with their ideology.
- *Expansion of surveillance:* Expansion of surveillance capabilities to include the gaming industry and player data.

Policy trends assessment

Policymakers acknowledge that video games have many positive outcomes for entertainment, expression, communication, and learning. The European Games Developer Federation (EGDF) and Europe's Video Games Industry (ISFE), for example, draw attention to the numerous advantages that video games offer to consumers, including those related to mental health, as well as the industry's role in technological innovation and the significance of the sector for the EU's cultural and creative industry (Lambert, 2023). However, video games also have the potential to be powerful platforms for spreading extremist ideologies, grooming vulnerable individuals, promoting hate speech, and disinformation. As gaming and game-adjacent platforms are not subject to the same levels of regulation as mainstream social media platforms or cryptocurrencies, they are vulnerable to abuse by hostile states, terrorists, extremists, and other criminal groups (EU Counter-Terrorism Coordinator, 2020, p. 3).

There is little consensus in the policy literature about whether online gaming platforms are taking sufficient action and whether those actions are having the intended effect (Schlegel, 2021b; Gallagher et al., 2021; Lakhani, 2021; Thomas, 2021; Vaux et al., 2021). In their draft report on consumer protection in online video games, the European Parliament's Committee on the Internal Market and Consumer Protection emphasises the need for the video games industry to adopt suitable measures and tools to protect users from harmful content in accordance with applicable national and EU legislation (European Parliament, 2022, p. 7).

The Digital Services Act (DSA) makes provisions for Very Large Online Platforms (VLOPS) that may by extension apply to some video game and game adjacent platforms. Future policy development in this area is likely to be inspired by how the DSA handles VLOPS, and especially the input of companies that are both in gaming and social media (e.g., Microsoft and Google/YouTube). Microsoft are especially well-placed to influence public policy, following years of participation in the Code of Practice on Disinformation, DSA, and their leadership for the Paris Call. It is likely, based on regulatory developments targeting social media, that in the coming years the video game industry will be expected to voluntarily submit regular threat assessments and risk mitigation plans, publish transparency reports about content moderation (including the capability for an independent audit mechanism), and make provisions for access data for researchers. Note that additional platform-specific policy details are covered in Chapter 4.

Examples of policies that have been implemented to mitigate extremism, grooming, and hate speech in video games as well as a means for countering malign foreign interference and information influence include:

- *Content moderation.* Many social platforms for video games, such as Discord, Twitch, YouTube, and DLive, have policies and procedures in place for moderating user-generated content, including steps to remove or flag content that is extremist, grooming-related, or involves hate speech. These policies may be enforced by in-house moderation teams or by third-party contractors. Before September 2018, discussion

board content moderation on Steam was left up to the game developers' judgement. Following the moderation update, when a player flags a forum post or discussion thread in the community, it is added to a queue for Steam's in-house moderation team to review. Any posts that are reported as being in violation of Steam's Community Guidelines should be reviewed and removed (Steam, 2018b). Following the moderation updates, over 170 games have been taken off the platform, and in December 2019, Valve removed 50 instances of Nazi-related user content, in compliance with a request from the German government (Anti-Defamation League, 2020). Similarly, following the Capitol storming in January 2021, DLive increased content moderation on far-right users. These steps included measures such as demonetisation of accounts, enforcing stricter content moderation policies, banning influential figures, and conducting content moderation of all "X tag" channels with significant viewership (channels tagged as being primarily political) (Lakhani, 2021, p. 18).

- *Age ratings.* A specific vulnerability of the video game domain is the potential audience of children who may not be adequately prepared to deal with threat scenarios. To assist parents and other adults in making knowledgeable choices about which games are appropriate for kids, video games have a content rating system. These systems are often sponsored by or affiliated with governments. When games are being prepared for their distribution in other nations, rating verification and approval are a part of the localisation process (Foust, 2022). Examples of video game content rating systems include the European PEGI system, the German USK system, and the ESRB system used in Canada and in the US. More than 30,000 video games have been categorised by PEGI since 2003. 2019 saw the release of the PEGI App, which makes it possible to review the ratings and content of games with the PEGI rating on a smartphone. Users can use it to search the PEGI database for the most recent video game and app rating classifications (EDGF & ISFE, 2022, p. 17–19). Some European countries have already made the PEGI system a legal requirement and the European Parliament's Committee on the Internal Market and Consumer Protection has urged the Commission to investigate the possibility of enshrining the PEGI system in EU law (European Parliament, 2022, p. 7). Additionally, they make the case for the creation of an identity verification system that could be used across Europe that can also certify the privacy of players' data. This system would allow players' ages to be verified (ibid, p. 9). Age verification is one of the current policy tools that could develop into a means of managing access both to gaming content and game-adjacent functions where propaganda is spread.
- *Parental controls.* Involving and educating parents about their children's gaming activities is one of the current policy mechanisms under discussion. Several video game platforms provide parents with tools to keep an eye on their children's video game playing habits. These controls can be used to block or restrict access to certain content. In addition to age limits, these control tools can include limits on online spending, playtime, and tools to restrict the players' online interactions

(EDGF & ISFE, 2022, p. 21-23). The European Parliament's Committee on the Internal Market and Consumer Protection notes that parents might find it challenging to use such tools, which lower their efficiency. They argue that spending excessive amounts of time playing online video games can have a detrimental effect on social interactions, including school drop-out, physical, and mental health issues, and poor academic performance, and call for the overall improvement of child and adolescent supervision systems (European Parliament, 2022, p. 6).

- *Regulations to avoid addiction.* Numerous studies have revealed a connection between loot boxes and addictive gambling behaviour (see overview by Close & Loyd, 2021). Regulations for in-game purchased and loot boxes vary by country and region. In some countries, such as the Netherlands, loot boxes with real-world value have been banned outright as a form of gambling. Despite the Belgian Gaming Commission's recommendation for criminal prosecution against illegal loot boxes in 2018, research discovered that numerous companies disregarded the ban and easily found ways to evade compliance with the law (Xiao, 2023). In 2021, the German Bundestag adopted a new Youth Protection Act in which these concerns were raised. Following the act, "interaction risks", such as in-game transactions and loot boxes had to become more visible, adopting descriptions similar to the International Age Rating Coalition (IARC) system (The German Games Industry Association, 2021). In other countries, such as the United Kingdom and the United States, loot boxes are not regulated as gambling. In 2023, The European Parliament voted for the Commission to investigate the impact of loot boxes and in-game purchases and act if necessary. They also urged developers to avoid creating addictive games (Batchelor, 2023). In 2019, the UK's Department for Digital, Culture, Media & Sport released the findings of its "Immersive and Addictive Technologies Inquiry". The report recommended that loot boxes with an "element of chance" should only be purchasable with earnable, in-game credits and not real money. It also pushed for better labelling and age verification tools for games containing loot boxes, particularly for younger people who are more susceptible to addiction (Gardner, 2019). Similar requests have been made by other actors, including the #LidOnLoots campaign1, led by the Gambling Health Alliance (GHA), calling for loot boxes in video games to be classified as a form of gambling and have age ratings.
- *Education and awareness:* Many organisations and initiatives have concentrated on educating players and other stakeholders about the risks associated with extremism, grooming, information influence, and hate speech in video games, as well as on promoting positive alternatives to such content. These efforts aim to explain how to activate parental control tools available on every device and to promote the added-value benefits of playing video games, such as in education. Such initiatives include Fråga, Prata, Spela[5] in Sweden, The Good Gamer[6] in Spain, RuleTheGame[7] in the Netherlands, Ask about Games[8] in the UK, and Tutto sui videogiochi[9] in Italy (EDGF & ISFE, 2022, p. 23).

[5] http://www.fragapratаspela.se
[6] www.thegoodgamer.es

Recommendations

Below is a series of draft recommendations about how to strengthen the resilience of the gaming domain to malign influence.

1. In all framing and discussion of the problem, fundamental freedoms such as freedom of speech and expression must come first. Nobody should want to take away games or 'crack down' on games, gamers, or the gaming industry. The question is rather how does one conduct research and analysis of what is happening in these spaces in a manner consistent with fundamental freedoms?
2. It is essential to learn lessons from social media platforms when approaching the gaming industry on these issues. In particular, lessons from voluntary agreements such as the EU Code of Practice on Disinformation and GIFCT reveal successes and also missteps that do not have to be repeated. Gamers and industry should be part of the solution, and not positioned as the problem.
3. Respect the early movers in this space, that is to say tech giants such as Microsoft who have played a key role in countering information influence on social media and who are well-positioned to exert positive influence in the gaming domain.
4. Countermeasures should be designed as a partnership between industry, players, and governments in a spirit of dialogue aiming to avoid major threats and harms such as a '2016 moment' for video games.
5. More research on all aspects of gaming and information influence is needed. This means that access to data for researchers should be a priority issue for this policy area. Researchers could begin with targeted studies focused on known issues, including TTPS raised in this report.
6. One of the most important methods that the industry could use to fast-track research is to allow for self-submission of user data to research groups, for example by integrating mechanisms for gamers to flag content on gaming and game-adjacent platforms. The model may be compared to Netvizz and NYU Ad Observatory on Facebook, both of which were eventually banned by the platform owner. It is essential to ensure goodwill agreements at an early stage of cooperation to guarantee that such initiatives have the support of industry and don't get deplatformed.
7. There should be more support for exchanging best practice between Trust and Safety teams in different sectors to ensure that the gaming industry is at the cutting edge of user protection. This includes areas such as threat intelligence, content moderation, data sharing, risk assessments, and auditing. In particular, the major gaming platforms should be encouraged to develop in-house T&S capabilities if they do not have them already.

[7] www.rulethegame.nl
[8] www.askaboutgames.com
[9] www.tuttosuivideogiochi.it

8. It is important to acknowledge that gaming is not ringfenced and that potential harms are not gaming-specific. Gaming should be considered alongside traditional media, and in particular film, television, and internet-based content; new interactive technologies such as the Metaverse, AR/VR, AI and others; as well as alternative parts of the internet where gamers may interact or where gaming provides a common language, such as social media, porn, shopping, and other places where gaming cultures seep into the language. This means that, while we have identified more than 40 TTPs related to gaming, other TTPs from other domains will also be relevant; furthermore, a cadre of cross-platform TTPs will also be needed.
9. From an intelligence perspective, it should also be acknowledged that gaming is a further challenge to the traditional stovepipes that separate analytical fields from one another. For example, it may be impossible in some gaming-related instances to distinguish between hybrid, cyber, influence, and military methods and objectives.

2 | Research on cognitive influence

2. Research on cognitive influence

The practice of playing video games is almost as old as computers themselves. In the United States and Japan, the first games were developed in the 1960s. By 1982, the gaming industry had a higher turnover than the Hollywood film industry and pop music industry combined (Rogers & Larsen, 1984). Today, the video game industry is one of the largest global cultural industries, with considerable social significance (Lakomy, 2019, p. 384). The global video game market continues to outpace both the global film and music industry (Foust, 2022). Revenue in the video games sector is likely to reach 221 billion US$ globally in 2023: mobile games accounted for over 75 percent of this revenue in 2022. In Sweden, half of all men (49 percent) and over a third of all women (37 percent) aged 16–84 played video games in the past 12 months in 2021 (Folkhälsomyndigheten, 2022).

Throughout the 50-plus years that video games have been part of popular culture, there has been the assumption that they are capable of profound influence. Delwiche (2007, p. 92), for example, argues that "video games have the potential to shape attitudes and behaviour in ways that Goebbels could never have dreamed". Foust (2021) notes that games are a contested space for political dialogue, in which "governments and corporations, journalists and activists, and players of every stripe, are competing to tell stories and shape perceptions about the world." Fears about addictive gameplay, excessive violence, and disproportionate persuasion belie an expectation of cognitive influence, both upon groups and individuals.

Arguably, the biggest concern has been whether playing video games encourages violent behaviour, especially among children and teenagers. Motion capture games which depicted graphic violence, such as 1992's Mortal Kombat, saw significant media attention and public scrutiny. This prompted two US congressional hearings on the topic of violence and video games in 1993 and 1994 (Crossley, 2014). Shortly after, a voluntary age restriction system similar to motion pictures was introduced. Since the 1999 Columbine High School shooting, a sizable body of literature exploring the potential connections between gaming and violence has accumulated (Campbell, 2018; American Psychological Association, 2020).

The connection between violent or aggressive video games and violent behaviour among young people remains a contested topic. Numerous studies on the impact of video games on youth delinquency (DeLisi et al., 2013), societal violence (Ferguson, 2015), school shootings (Crump, 2015), and the acceptance of aggressive behaviour (Funk et al., 2003; Beck et al., 2012) have indicated that those with higher levels of aggression choose to play violent

video games more frequently (Przybylski et al., 2009). Furthermore, they suggest that playing video games can have neurological effects on players (Engelhardt et al., 2011) such as normalising violent behaviour (Lin, 2013; Greitemeyer, 2014).

The American Psychological Association (2020) states that while there is a well-established link between violent video games and aggressive behaviour, empirical research finds little to no evidence showing a direct correlation between playing video games and committing violent acts. However, video games may have a mediating effect when considering other factors such as mental illness, family situation, loneliness, and school situation. The findings, according to Schlegel (2020, p. 5), indicate that violent video games could have a negative impact on players even though there is no direct and causal link between them and violent behaviour.

More recently, an increasing number of studies have built a body of evidence on the potential advantages of video games use (Jiow et al., 2019, p. 5). Various studies have, for example, found evidence of that video gaming may foster a stronger social bond between family and peers (Kowert & Quandt, 2016), and develop the players' problem-solving skills (Jiow et al., 2019, p. 5). Studies have shown that video games can combat cognitive decline associated with aging, improve information processing and sustained attention, and offer lasting cognitive benefits that persist for months after the training (Granic et al., 2014). Alongside these positive outcomes, there are also studies suggesting that excessive video game use can result in negative consequences such as mood disorders, problems with social interactions, and addiction (Jin et al, 2021).

The addictive potential of video games has long been a subject of ongoing debate among researchers and health professionals. A comprehensive review of more than 250 research articles about the adverse consequences of excessive gaming led to the inclusion of video game addiction in the American Psychiatric Association's Diagnostic and Statistical Manual of Mental Disorders in 2013 (American Psychiatric Association, 2013; Dervesh et al., 2020, p. 2). The condition requires a preoccupation with gaming, symptoms of sadness, anxiety, and irritability when gaming is taken away, unsuccessful attempts to quit, giving up on other enjoyed activities due to gaming, and the use of gaming to relieve negative moods. In 2018, the World Health Organization (WHO) included Gaming Disorder in the 11th revision of the International Classification of Diseases.

The question of whether video gaming should be classified as an addiction or mental disorder is, however, highly debated and an area of increasing research (Sherer 2023). One shortcoming is a lack of consensus over the diagnostic criteria (Jiow et al., 2019, p. 2). For example, Darvesh et al (2020) discovered a total of 160 studies that utilised 35 different diagnostic methods for gaming-related mental disorders. A 2017 study on the validity and reliability of the criteria for video gaming addiction found that the percentage of individuals qualifying for the disorder is extremely small (Przybylski et al., 2017), yet more recent studies suggest that the prevalence of addiction might be very high (Gao et al., 2022). Several studies have found a significant rise in the symptoms of video game addiction during the pandemic (Sherer, 2023). Estimates of the prevalence of gaming-related mental disorders

therefore vary massively: from 0.21% to 57.50% in general populations, 3.20% to 91.00% in clinical populations, and 50.42% to 79.25% in populations undergoing interventions for severe cases (Darvesh et al., 2020).

This chapter explores some of the ways in which video games are believed to produce cognitive influence, whether those effects are positive or negative. First, the chapter outlines the revenue models that dominate the industry, and how they relate to some of the more controversial issues of player health and well-being. Following that, the chapter introduces some aspects of game design and the social functions that accompany some forms of gaming. Finally, the chapter discusses some of the ways in which games have been used to represent different social groups, advocate for social, cultural, and political issues, and attract players to certain careers or lifestyles. Since research is in general inconclusive about positive and negative effects of games on gamers, this chapter focuses on providing examples of how games are and have been employed, rather than making assumptions about their overall impact on gamers.

Industry & revenue models

Gaming is a profit-driven enterprise. However, in the past decade, the video-game sector's strategies for generating revenue have changed. Retail sales, for example, which represented 98% of the company Ubisoft's sales in 2010, accounted for less than a third of their total sales revenue in 2020. Instead, game publishers have expanded their revenue sources beyond retail to now include strategies such as microtransactions, downloadable content (DLC), and Season Passes where the game developers and publishers extend the life of the game by offering additional content for an additional fee (Zhang, 2020). In many respects, the compelling elements of gaming have been further finetuned to support more effective revenue streams.

Prior to the 2000s, the predominant model in the gaming industry was Pay-to-Play (P2P), where developers and publishers earned revenue through game sales. Arcade games, for example, were sometimes referred to as "quarter munchers" because their high difficulty and urge for "one more try" required the continual depositing of coins to keep playing. Games for home computers and consoles were typically purchased outright, with a portion of the cost going to the platform owner (such as Sega, Nintendo or Sony) as a license fee. Generic games were often made more attractive through licensing deals with movies and TV shows, allowing them to be marketed to broader audiences.

More recently, the industry has partly shifted from P2P to Free-to-Play (F2P) models. Instead of solely generating revenue through retail purchases, games may be funded through advertisements, or allow users to unlock certain elements of the game, bonuses, or the full version of the game for a fee (Dataspelsbranschen, 2022, p. 62). As such, F2P games rely on microtransactions where the player has the option to spend money on in-game content instead of paying upfront costs as with P2P-games. Microtransactions were introduced in games in the early 2000s as in-game purchases that unlock content or offer advantages for the players in exchange for a small fee (Ball & Fordham, 2018).

Loot boxes are virtual in-game items that can be purchased and contain randomised rewards (Close & Loyd, 2021, p. 2). They are a microtransaction similar to trading cards in the sense that the contents of a purchased pack are unknown until they are opened; the reward may be very rare and valuable, or some common items. Many games, and particularly those with F2P models, have allowed players to purchase loot boxes as a way of gaining in-game advantages. Due to their structural and psychological resemblance to gambling, loot boxes have been subject to growing legal, academic, and media attention. Loot boxes have become a controversial issue in the gaming industry due to concerns about their similarity to gambling and their potential for exploitation of vulnerable players, particularly children. Regulations for in-game purchased and loot boxes vary by country and region. As mentioned earlier, in the policy section, numerous studies have revealed a connection between loot boxes and addictive gambling behaviour (Close & Loyd, 2021).

One of the most common strategies for generating profit in F2P games is to use advertisements. Advertisements allow the game developer to sell both space within the game and the data generated by players. Games such as Angry Birds 2 allow free play, additional tries, or additional levels, in exchange for watching ads. Bernevega and Gekker's (2022, p. 63) analysis demonstrates that user data extracted by gaming companies is not only used for internal purposes; in many cases, it is also shared with third parties such as service providers who offer payment processing or assist with data management, business partners such as external game developers who offer their products through the publishers' digital platforms, and marketing partners who utilise collected data for targeted advertising. Similar to digital advertising giants such as Facebook and Google, game companies aim to leverage user-generated data to place ads in front of the "right" audiences. The companies match users with advertisers based on specific specifications, mobilising user data to maximise profits (Egliston, 2022).

Closely related to the F2P model is the Play-to-Earn model (P2E). P2E allows players to play a game and earn money, for example cryptocurrencies, from their in-game labour. The model has become increasingly popular during recent years. The psychology behind this approach revolves around rewarding players as they invest more time into the game. They receive an incentive or reward for their playing time in the form of digital assets with the potential for value appreciation (Revoredo, 2022).

A further revenue model is competitive gaming, also known as Electronic Sports or e-sports (Luxembourg House of Cybersecurity, 2022). For a game to be classified as an e-sport, it requires the competitors to play against each other and the outcome should be based on the players' performance. Thus, gambling, and other online games such as poker are not e-sports (Svenska E-sportförbundet, n.d.). The term e-sport is often conflated with "online gaming," but represents only one facet of the broader online gaming landscape. In 2021, the global market size of e-sport reached $2bn (Grand View Research, 2021) and is expected to reach $5.48 billion by the end of 2029. The e-sport industry has experienced enormous growth, mainly as a result of the expanding audience. As of 2023, e-sport has a global audience of over 532 million people, a number estimated to reach 640.8 million by 2025 (Ruby, 2023). Prize money for competitions can be in the millions of dollars.

Game design

Game design encompasses the overall process of creating a video game, including development of the gameplay, environment, storyline, and characters. System design is where developers craft the rules and mathematical patterns that underlie gameplay mechanics. Content design involves creating the characters, items, puzzles, and missions that populate the game world. Game writing is yet another important component of video game design, involving the crafting of dialogue, text, and overall storylines. User interface (UI) design involves the construction of the user interactions and feedback interface, including menus and heads-up displays (Brathwaite & Schreiber, 2008, p. 5).

Storytelling and narratives play a crucial role in many video games, as they help to create a sense of immersion and provide a context for the player's actions. Many modern games use interactive elements to engage the player in the narrative. Interactivity is how the player actively participates in, and experiences, the story, mechanics, and environment of a game (Sautman et al., 2017). Interactive elements in games range from simple button pushes to move objects through to branching dialogue choices, pathways, or moral decisions with bearing on the narrative. Choices made at the game design, system design, and content design stages have a huge impact on the extent to which players become engaged with a game.

Interactivity also takes place by facilitating contact between players. Many video games feature local or online multiplayer options. Massive Multiplayer Online Games (MMOs) allow players to interact, collaborate, and compete with dozens (many first-person shooter [FPS] games, such as Counter-Strike), hundreds (multiple-shard MMOs, such as World of Warcraft), or even thousands (single-shard MMO Eve Online) of users within the same game world (Lakomy, 2019, p. 386).

The online gaming landscape consists of several actors. These include content distributers, such as the Google Play Store and Steam; streaming and monetisation services, such as Twitch and YouTube Gaming; and hardware developers such as Microsoft, Sony and Nintendo, who build and offer subscriptions to the technical infrastructure that is required to play the game. Online gaming can be tribal; typically one is either for Playstation or Xbox, Call of Duty or Battlefield, Mario or Sonic, and this sense of community and belonging generates rivalries that can be greater than those within a competitive game.

In the past decade, the mobile gaming industry has experienced enormous growth, emerging as one of the most rapidly expanding sectors in the gaming industry (Vega, 2023). Mobile gaming apps refers to games specifically designed for mobile devices, such as smartphones and tablets. These apps cover a broad range of genres and can be accessed through stores such as Apple App Store for iOS devices and Google Play Store for Android devices. The popularity of mobile gaming apps has increased due to the convenience and accessibility of playing games on mobile devices. In 2022, the annual Google Play game revenue reached $31.3bn and Apple App Store game revenue reached $50bn. The mobile gaming industry is rapidly growing and by 2020, consumer spending on mobile games surpassed that of PC and console

games, and it is expected that the gap continues to widen in the future. In 2021, mobile game consumers spent a total of $89.6bn. Since 2017, China has held the top position of consumer spending, followed by the United States and Japan. Role-playing games (RPG) have been the most popular genre in between 2019-2021, followed by strategy, puzzle, and casino. RPG made up almost $25bn of the $89.6bn total game spend (Curry, 2023).

The emergence of mobile gaming has impacted the gaming industry and created new opportunities for game developers to create games optimised for mobile devices. It has also enabled the rise of cross-platform games, enabling players to play on both mobile devices and traditional platforms (Vega, 2023). As such, there has been an increase of game companion apps, which are apps designed to enhance the gaming experience of the main game, providing additional features such as mini-games, maps, tutorials, and other resources. Examples of such apps are FIFA Ultimate Team (FUT), in which players can manage their team from their phones, including buying and selling players, and setting up game tactics, and Fallout Pip-Boy, which enables players to have a second screen experience for the Fallout 4 Game.

Technological advancements in the form of Virtual Reality (VR) and Augmented Reality (AR) enable more advanced interactive game elements. Often known collectively as immersive gaming, specialist peripherals aim to give the player intensified experiences of presence, immersion, and embodiment (Lockheed Martin, 2020). VR, for instance, can integrate eye-tracking systems into headsets. This innovative form of interactivity allows game events to be triggered or delayed based on where the player looks within the virtual environment, or if they blink (Pagan, 2019). VR games use headsets and other equipment to create a fully immersive 3D environment that the player can interact with as though they were 'there' (Lutkevich, 2023). Subsequently, VR video games have also been developed for training purposes and clinical treatments (e.g., for psychiatric diagnoses such as autism and post-traumatic stress disorder), with positive results.

Functions supported by AR include detection and tracking of the real-world environment using advanced sensors such as cameras, microphones, and GPS, allowing game visuals and audio to be overlaid on top of reality as one views it. Building on the foundations of AR gaming, mixed reality (MR) and extended reality (XR) take this concept a step further by enabling real-time feedback between the player's physical environment and the virtual game world (Rosenberg, 2023). The "gamification" affordances of AR have legitimate real-world applications; for example, many smart vehicles now project AR hubs onto windscreens so that drivers can see their speed, maps, and other dashboard information without looking away from the road.

Social functions

Video game audiences have grown significantly as a result of the expansion of online streaming, which has led to the development of major game-adjacent platforms. On Twitch, for example, well-known online streamers can broadcast commentary and live feeds of the games they play to a subscriber base of millions (Foust, 2021). Users can live-stream video content on sites like

YouTube, Twitch, and DLive, with options for revenue creation through advertising, subscriptions, or donations (Squire, 2021, p. 1). Formats include videos, livestreams, interviews, chats, books, documents, memes, and talk shows (Lakhani, 2021, p.10).

There is doubt within the research literature about whether game-adjacent platforms offer sufficient content moderation (Schlegel, 2021b; Gallagher et al., 2021; Lakhani, 2021; Thomas, 2021; Vaux et al., 2021). Some argue that collaboration with gaming platforms is required across the ecosystem, including social media platforms, in order to exchange knowledge, experience, and best practices (Lakhani, 2021, p. 16). With many gaming rigs using multiple screens that link video and text-based social functions to the gaming experience, as well as spoken chat functions within cooperative and competitive online games, social functions are a major component of contemporary gaming. While there are a handful of gaming industry actors who are also active in social media (e.g., Microsoft, Google/YouTube), in general there is at present little consistency in how game-adjacent platforms are viewed in comparison to social media.

Representation

Representation in media, including video games, helps to create a sense of community and belonging. When we see people like us in the media we consume, it makes us feel seen and understood. Representation of different races, genders and sexualities in video games can make the experience more immersive and enjoyable, whether gamers seek to play as an avatar with similar characteristics to them, or entirely different.

There is often a misconception that it is only younger men who play video games. While the industry and production of games is dominated by men, according to statistics from the US over 40 percent of players are female; similar numbers are valid in many other countries. Still, video games have a rocky history with diversity and inclusivity. Studies on representation in video games show that non-white women have been largely under-represented in video games (see Burges et al., 2011; Mou & Wei, 2009; Russworm, 2017). Almost 80 percent of the main characters in the 100 most-sold video games released between 2017 and 2022 were male, with 55 percent of them being white (Webb & Davies, 2022).

Studies indicate that white video game characters often are represented as being drawn to violence, crime, and physical prowess (Burges et al., 2011), and that black characters often appear more one-dimensional with less intellect than their white counterparts (Harris, 2016). Video games often adhere to traditional gender roles and binary characters. For instance, female characters are often portrayed as submissive and sexualised with less narrative importance compared to male characters (Friedberg, 2015). In addition, games tend to sexualise non-white women characters more than white women characters (McCarthy, 2015). Studies have furthermore suggested that characters who are marginalised in terms of their sexual orientation, gender identity, or intersex status (MOGAI) are often portrayed as deviant figures in video games, used mainly for comedic purposes or as secondary antagonists in the story (Talbert, 2016).

On game-adjacent platforms, harassment of females has at times become a scandal for the industry at large. In 2014 and 2015, an online harassment campaign that targeted female game developers and critics came to be known as #GamerGate (Milburn, 2018, p. 23). The movement originated from a dispute over allegations of ethical violations by a female game developer, alongside more general misogynistic grievances about feminism and representations of progressive social issues in video games (Kaplan, 2014). The harassment campaign included the hijacking of social media accounts, threats of murder and rape, and doxing. These threats escalated until several public figures in the video game industry were forced to leave their homes and cancel public appearances. Anyone who criticised sexism, racism, and homophobia in video games risked becoming a new target (Milburn, 2018, p. 163). #GamerGate received significant media coverage and led to a larger discussion on online harassment and misogyny in the gaming industry.

The representation of diversity and inclusivity in video games is constantly evolving, and there have been progressive developments in recent years. For example, in 2017 Xbox One Avatars were updated to include a range of new features including the ability to use wheelchairs, prosthetic limbs, and even pregnancy in the avatar design (Prell, 2017). Following movements such as #MeToo and Black Lives Matter, more focus has been placed on social inequalities in video games (Webb & Davies, 2022). Representation is also crucial in gaming streams, where female-identifying gamers make up 35 percent of streamers on platforms like Twitch (Webb & Davies, 2022).

Advocacy

The concept of using games for good has gained significant attention in recent years as gaming technology has become more advanced and widespread. Video games have the potential to be valuable educational tools as they can convey values and ideologies, both intentionally and unintentionally (Flanagan, 2009, p. 223). In recent years, several games that promote positive social, educational, and health-related outcomes have been published. These games can include raising awareness and promoting positive behaviours relating to health (Zombies, Run!, Ring Fit Adventures, Just Dance), education (World Rescue, Endless Alphabet, National Geographic Challenge), or cultural awareness (Never Alone, Spirit Lake: The Game, Thunderbird Strike). Several studies have demonstrated the effectiveness of video games in developing empathic behaviour among players and delivering educational material (Hasler et al., 2014; Belman & Flanagan, 2010; Darvasi, 2016; Ritterfeld et al., 2009).

Political campaigns have also started to leverage the potential of video games and game-adjacent platforms for innovative fundraising methods as well as to reach a broader audience. Platforms like Twitch allow politicians to set up channels, stream events, and engage with supporters while accepting donations. In addition, partnerships with popular video game developers can lead to in-game events or merchandise that can help raise funds for campaigns. The use of video games provides a unique platform to raise awareness about the candidates campaign, as seen in the 2020 US Presidential Election where, for example, the Joe Biden campaign used

Animal Crossing: New Horizons (Reymann-Schneider, 2020) to create a virtual field office and Fortnite to create the "Built Back Better with Biden" map (Dhar, 2020).

According to some, video games are powerful providers of ethical and cultural discourses (Rodríguez Espínola, 2021; Perez Latorre, 2015, p. 417). While historically representations of, for example, indigenous groups featured misrepresentation and negative stereotypes (Wheeler, 2014; Espínola, 2021), video games are increasingly seen as an opportunity for self-representation. One example is the award-winning game Never Alone, developed in partnership with the Cook Inlet Tribal Council (CITC) and E-Line Media, revolving around the culture of the Alaska Native community. The game features a story passed down through the oral storytelling tradition including 26 "Cultural Insights" that players can unlock through gameplay. The game is a cooperative puzzle-platform game that aims at celebrating, extending, and raising awareness. E-Line Media describes the game as "… not a game made about the Alaska Native people, it is a game made with the Alaska native community" (Gershenfeld & Angst, 2021). Although primarily marketed as a consumer entertainment product, it has been distributed to schools with a classroom guide in Alaska and incorporated into curriculums worldwide. Never Alone has also been showcased in many museums, including the Denver Art Museum and the Chine Academy of Fine Arts (ibid).

This War of Mine is a survival-themed video game developed by 11 Bit Studies, set in a fictional war-torn city in which the player takes on the role of a civilian trying to survive during a modern conflict. The game aims to raise awareness of the harsh realities of war and the impact it has on civilians (Webber, 2016). Similarly, the International Committee of the Red Cross (ICRC) developed a mini game within the popular video game Fortnite to raise awareness about the devasting consequences of war, educate players about the challenges faced by humanitarian workers, and the importance of protecting civilians during armed conflicts. The mini game, Liferun, launched in 2020 and includes a link to the ICRC's website[10]. The thing that these games have in common is use of the medium of video games to create meaningful and educational storylines that encourage the player to engage with social issues.

In early May 2023, Finnish newspaper Helsingin Sanomat wrote about an information campaign they had conducted in collaboration with game designers. The target group was young Russians. The aim was to increase knowledge about the Russian war in Ukraine. The method was unique and innovative, a consequence of the fact that basically all journalistic and social media platforms in Russia are controlled by the Russian state and used for propaganda. The campaign was launched inside a very popular video game, Counter-Strike, which was not influenced, forbidden or controlled by the Russian state. Inside the game was a secret room where players would be exposed to real news about the war – the actual number of Russian soldiers killed in action, the massacre of civilian Ukrainians in the city of Bucha and about the Russian missile that killed a whole family, including a three-month old baby, in Odessa[11].

[10] https://www.icrc.org/en/fortnite-liferun
[11] https://www.hs.fi/ulkomaat/art-2000009555855.html?share=745dc6c3c84d9d841cc3579d8d30b943

The proliferation of online disinformation and extremism in recent years has highlighted how important it is for individuals to be able to identify and critically evaluate the content they come across online. One way to improve people's ability to detect disinformation and extremism is through the use of videogames. Games can provide a fun and interactive way to learn about the tactics and techniques used by those who seek to spread harmful information and ideologies and can help players to develop the skills and knowledge needed to identify and mitigate the impact of this content. Various video games have been designed with the goal of training players to detect disinformation and extremism online. These games function as a tool for improving media literacy and critical thinking skills. Adventures of Literatus, for example, is an educational, hidden object and fantasy adventure game. Players take on the role of Prince Literatus, who must embark on an information-gathering mission to free his truthful lady and shield the kingdom from confusion and false information. Along the way, Literatus encounters trustworthy, dishonest, and dubious members of the media and must solve several media and information literacy (MIL) puzzles (Plaum, 2020). With guidance from a seasoned disinformation "mentor", the game Bad News uses the classic choose-your-own-adventure format to put players in the role of a fake news writer, populist, or propagandist on a social media platform similar to Twitter. The aim is to gain as many followers as possible while disseminating information that ranges from highly dubious to downright offensive. The goal of the game is to "vaccinate" players against false information (ibid).

Recruitment

The Pentagon has used video games for recruitment for 20 years and undoubtedly sees gamers as a high-value outreach target. The most well-known of these initiatives, *America's Army*, is a series of first-person shooter game (FPS), first released in 2002 (Foust, 2021). The Army has since released regular updates that include fresh training materials, new maps, and bug fixes (Nieborg, 2004, p. 1) and as of 2022, when the US Army announced it would shut down the series, there had been over 41 one versions of the game (Chalk, 2022). According to Schulzke (2013, p. 2), America's Army is likely the most successful attempt to use video games for strategic communication,

> *"30 percent of all Americans aged 16 to 24 had a more positive impression of the Army because of the game and, even more amazingly, the game had more impact on recruits than all other forms of Army advertising combined".*

The videogame has, however, been criticised for contributing to a militarisation of society, and blurring the line between real and virtual violence (see Allen, 2011; Salter, 2011; Schulzke 2013). This has drawn criticism from parental organisations, journalists, and academics (Souri, 2007, p. 543). U.S. Army colonel Casey Wardynski emphasised the importance of attracting gamers while they are still young because

> *"If you don't get in there and engage them early in life about what they're going to do with their lives, when it comes time for them to choose, you're in a fallback position."*
>
> (Ryan, 2004)

There are several examples of how video games have been used as training platforms and for recruitment purposes, allowing organisations to train and identify necessary skills in candidates. In 2020, the UK Ministry of Defence and Defence and Security Accelerator announced the launch of a new virtual reality training platform for the UK Armed Forces, building on the same gaming engine as the popular game Fortnite (Ministry of Defence & Defence and Security Accelerator, 2020). Another example is the online puzzle-game CryptoChallenge, a game developed by the US National Security Agency (NSA) to test potential candidates' ability to decipher codes, solve cryptograms, and their analytical skills (The National Security Agency, 2011). Similarly, the US Navy has used the cryptography puzzle-game Operation Sleeper Shark as a recruitment tool in which a series of desirable skills in candidates can be identified (Wenz, 2015).

3| Research on threat vectors

3. Research on threat vectors

The first chapter of this report outlined the main threats and vulnerabilities that video games present from the perspective of foreign information manipulation and interference. It drew upon a typology of known TTPs used by threat actors in the video game sector, with an emphasis on outlining the tactics and techniques used. The second chapter has given an overview of the gaming industry, including some of the main debates about the types of cognitive influence – positive or negative – that games possess according to research. This chapter builds on both previous chapters to provide a detailed assessment of current research on known threat vectors. It is focused on giving examples of where the potential for influence has been demonstrably exploited by threat actors, relying mostly on research into extremism. Chapter 1 emphasises tactics (how an anticipated goal is to be achieved) and techniques (a detailed description of the behaviour). This chapter demonstrates many of the procedures (detailed description of activities in the context of a technique) used by threat actors to exploit video games' affordances for cognitive influence.

Disinformation & misinformation

The use of video game assets to promote the spread of false information is well-documented and there is some evidence to suggest that it has been used deliberately to spread disinformation. For example, in 2017 the Russian Ministry of Defence published numerous posts in English, Arabic, and Russian on their Facebook and Twitter pages with photos claiming to be "irrefutable evidence" of cooperation between US and Da'esh combatants. The photos were debunked by Bellingcat (an independent group of researchers and citizen journalists), demonstrating that the images were, among others, cropped screenshots from the mobile game AC-130 Gunship Simulator (Higgins, 2017).
The first-person shooter game ARMA 3, originally created by Czech Bohemia Interactive in 2013 and modified in several versions since, has been used in mis- and disinformation incidents on multiple occasions. In 2018, footage published on YouTube was used in a video purporting to show a Turkish drone strike in Syria. In a press release the game publishers stated that,

> *"While it is flattering that ARMA 3 simulates modern warfare so realistically, we are clearly not happy that it can be mistaken for real battle footage and used as war propaganda"*
>
> (MSB 2017 in SOU 2020:29)

In response to its products being abused, the company has tried to flag fake clips and footage[12].

According to AFP fact check, a video claiming to depict the Israel-Hamas conflict was in fact footage taken from *ARMA 3* (AFP Sri Lanka, 2021). Similarly, a video circulated on Facebook in 2020 claiming to show the shooting down of a US military plane by Taliban militants in Afghanistan, and viewed nearly 9 million times, was also from *ARMA 3* (AFP Pakistan, 2021). After President Joe Biden announced the withdrawal of all American troops in September 2021, the video resurfaced. In 2020, AFP fact-checked and debunked similar videos claiming to show air strikes in Iraq[13], Azerbaijan[14] and Syria[15].

The Ukrainian MiG-29 pilot known as the Ghost of Kyiv gained significant fame on social media[16 17] for taking down invading planes during the beginning of the Russian invasion of Ukraine. However, the pilot was fictional, and the footage used in some online videos was taken from the 2013 video game *Digital Combat Simulator* (Eisele, 2022).

Historical appropriation

Video games often have military themes. First-person shooters (FPS), which simulate combat, bring in billions of dollars annually. The most well-known franchises, including *Call of Duty, Battlefield, Counter-Strike,* and *Halo,* have sold hundreds of millions of copies and incorporate elements of realism, science fiction, and inspiration from historical events (Foust, 2021). Numerous video games recreate incidents from recent or ongoing conflicts and present them as accurate accounts of those incidents. However, according to Schulzke (2013, p. 2), there are different ways that claims of realism can lead to confusion. Simulations of real-world events in video games always change key details. Perspective bias is established when events are typically shown from one side of a conflict, which players are encouraged to identify with.

An example of this is the Syrian video game developer Dar al-Fikr and their productions *Under Siege* in 2001 and *Under Ash* in 2003. Both games centre around the events of the Palestinian uprising. The games immediately became popular in the region and particularly in the Palestinian Territories. Although both games are based on historical events (Souri, 2007, p. 538), Arab gamers have been drawn to them because they allow players to neutralise Israeli dominance over Palestinians and gain an advantage in the resistance without any real-world repercussions. Dar al-Fikr considers them to be akin to documentaries, stating that "contents are inspired by real stories of Palestinian people, they were documented by United Nations records (1978 – 2004)". They explain on their website that,

[12] https://www.youtube.com/watch?v=qqW93ePJ82s
[13] https://factcheck.afp.com/clip-video-game-it-does-not-show-iranianmissile-strike-iraq
[14] https://factcheck.afp.com/clip-actually-shows-computer-generatedimagery-video-game
[15] https://factual.afp.com/no-no-es-una-defensa-rusa-en-siria-sino-unescenario-personalisado-de-un-videojuego
[16] https://twitter.com/Navjot1974/status/1498149086553583618?s=20&t=eTeYJub4Pi95Eh1LdLw-ug
[17] https://www.youtube.com/watch?v=SBBJ_JzV8u4

> *"When you live in the Middle East you can't avoid being part of the image. As a development company we believe that we had to do our share of responsibility in telling the story behind this conflict and targeting youngsters who depend on videogames and movies (which always tell the counter side) to build their acknowledgement about the world"*
>
> (Souri, 2007, p. 539)

Recruitment & mobilisation

The link between video games and violent extremism is a matter of growing concern for the European Union (EU Counter-Terrorism Coordinator, 2020; Schlegel, 2021b). According to a recent Radicalisation Awareness Network paper, extremists and terrorists, who are frequently forerunners in exploiting vulnerabilities in the digital sphere, are known to be active on gaming and game-adjacent platforms (Schlegel, 2021b). By introducing innovations faster than countermeasures are taken, they have had the opportunity to maintain a considerable digital advantage (ibid, p. 3).

According to Europol's annual European Union Terrorism Situation and Trend Report (2021, p. 56-57), the use of video games, gaming platforms and forums, as well as gamer channels, has been a growing trend for spreading right-wing extremist propaganda. In the report, the increased exploitation of the gaming landscape by terrorists and extremists is described as an unsettling trend. Right-wing terrorists are increasingly using gaming services and platforms to spread their propaganda to a younger audience (ibid, p. 5). In addition to spreading the right-wing extremist movement's ideology provides recruitment opportunities, and fosters relationships among its members. In addition, these activities function as a means of financing (ibid, p. 55). Some have gone so far as to claim that video games are essential to right-wing extremist culture. Terrorist manifestos have made use of video games, well-known games have been modded to adhere to extreme-right ideals, extremists have their own networks on gaming platforms, and misogyny emanating from these groups has significantly polarised and politicised far-right spaces (Lee, 2021).

There is, however, little research into the ways in which games and game-adjacent platforms may be used to radicalise groups and individuals (Lamphere & Bunmatong, 2021, p. 2). Research on the gaming–extremism nexus is largely theoretical. Although it is believed that terrorist organisations from a wide range of ideologies use gaming-related content and spaces, it is still in many cases unknown how, why, and to what extent they are successful in doing so (Schlegel, 2022, p. 6; Lamphere-Englund & Bunmathong, 2021, p. 10). Linda Schlegel (2020, p. 10) identifies some of the mechanisms through which games may promote radicalisation by satisfying psychological needs such as "feeling competent, feeling autonomous, and experiencing social relatedness". It is also noteworthy that games and game-adjacent platforms can support the spread of ideology, particularly for increasing "user

engagement with ideological contents" and "facilitate[ing] radicalisation by making the learning of ideological concepts engaging and 'fun'" (ibid, p. 11).

Most peer-reviewed research articles on gaming and radicalisation and/or violent extremism were released between 2010 and 2012 and were founded on earlier research (Lamphere-Englund & Bunmathong, 2021, p. 10). The Extremism and Gaming Research Network (EGRN) asserts that in the years following 9/11, a preliminary and limited research agenda about jihadist gaming was initiated. The research was, however, specifically focused on games, not gamification influences, game-adjacent platforms, or gaming aesthetics as such (ibid). As a result, the research has become outdated.

It would not be until the 2019 Christchurch attacks that a renewed interest was awakened (Mahmoud, 2022, p. 19). In 2022, the US Department of Homeland Security funded a research project focused on building resilience within gaming to extremist exploitation and radicalisation. A quantitative study published by one of the lead scholars in the project found "converging evidence that identity fusion may play a key role in the radicalization of gamers" (Kowert et al., 2022, p. 14). The study shows that gamers with specific personality attributes such as insecurity and loneliness are more prone to racism, sexism, and extreme behaviours online. The study compared the impact from two different games and showed that FPS *Call of Duty* had a much stronger effect on these personality types than a cooperative game such as *Minecraft*.

There are convincing examples of video games being used as recruitment tools by terrorist groups. For example, Hezbollah, Hamas, and Da'esh have used video games for influencing different target groups. In 2003, the video game *Special Force* was released by the Hezbollah Central Internet Bureau. The game depicts real Hezbollah operations during the Israeli invasion of Southern Lebanon in the early 1980s. The same real-world obstacles that Lebanese fighters faced, such as minefields, a large Israeli military presence, bad weather, and challenging terrain, must be overcome by players. One of the most well-known aspects of this game is the "training session", where participants can hone their aim before the "real" battles by conducting target practice on the Israeli prime minister at the time, Ariel Sharon, as well as other senior Israeli officials (Souri, 2007, p. 539).

In 2007, the Hezbollah Central Internet Bureau released Special Force 2 – *Tale of the Truthful Pledge*. In this sequel, the player assumes the role of a Hezbollah fighter in a recreation of the landscape and architecture of Southern Lebanon in the 2006 conflict between Hezbollah and Israel. By killing Israeli soldiers, the player earns weapons and points. "Through this game, the child can build an idea of some of the most prominent battles and the idea that this enemy can be defeated", said Sheikh Ali Daher, a Hezbollah media representative (Perry, 2007). In such examples, recruitment overlaps with historical appropriation.

In 2018, the Hezbollah Central Internet Bureau created a game similar to *Call of Duty* called *Holy Defense – Protecting the Homeland and Holy Sites* in which the main character engages in combat with Da'esh militants as well as non-believers (Barak, 2018, p. 2). Hezbollah claims that the goal of the game is to raise awareness among Shi'ite youth in Lebanon about their common Muslim identity, culture, and history (ibid, p. 3). The game's introduction reads:

> *"The game is not merely a game but rather a story that seeks to document one of the sacred stages of defense against the expansion of takfiri elements and against the American-Zionist plan. It is intended to document the many victims who fell in battle in this way"*
>
> (ibid, p. 2)

Games have been exploited by violent extremists for decades (Schlegel, 2020, p. 7). Although they have long been a component of the extremist "toolkit", the issue gained more attention with the rise of Da'esh, which made extensive use of gaming references and is said to have even created its own video game, Salil al-Swarim [The Clanging of the Swords] (Al-Rawi, 2018; Lakomy, 2019). The use of games and gamification elements has "migrated downstream" to other jihadist groups after becoming increasingly popular thanks to Da'esh (Dauber et al., 2019).

Jihadist organisations also use game elements in their recruitment and propaganda campaigns (Schlegel, 2021a, p. 4). Da'esh has prominently used footage from games like Call of Duty as well as imitated the aesthetics and point of view of first-person shooter games in their propaganda videos shot with helmet cameras. The group also launched an app designed to "playfully" transmit ideology to children through gaming elements (Dauber et al., 2019; EU Counter-Terrorism Coordinator, 2020, p. 7). In interviews and tweets, Da'esh propagandists have made references to video games. A study by Cori E. Dauber, Mark D. Robinson, Jovan J. Basliou, and Austin G. Blair (2019) sought to define the conditions under which a propaganda or recruitment video could be considered to be based on video game motifs and, second, to examine whether Da'esh's use of these motifs spread "downstream" to groups that have historically produced weaker video propaganda. The study concludes that other organisations copied the strategy, in the process improving both the quality of extremist propaganda and Da'esh's standing among its target audiences.

Extremist gaming cultures

Video games have a significant advantage over television, audio recordings, magazines, and books insofar as they are interactive. Immersion and personal involvement are made possible by well-designed games (Gee, 2005, p. 15). The interactivity and player agency that distinguish video games from other forms of media – namely, the active role players take in shaping the narrative in a compelling setting – may increase the degree of influence that playing these games has on players' perceptions and actions. Playing video games can completely engross players, enabling them to identify with the game characters and partially merge with their avatar (Schlegel, 2020, p. 4). According to Lakomy (2019, p. 385), this gives hostile actors new opportunities as it enables them to create a virtual world that is interactive and driven by a narrative or adventure that presents their worldview and ideology.

Studies on online radicalisation frequently concentrate on social media platforms like Facebook, Telegram, or Twitter (Weimann, 2010; Kaati et al, 2015;

Bloom et al, 2017). However, Schlegel (2020, p. 6) argues that it is reasonable to assume that games and gaming platforms can and do aid radicalisation processes. Games can for example allow players to practice specific skills in a risk-free environment that typically costs less than traditional instruction. In addition, the educational process is accompanied by enjoyment, which is even more beneficial in the context of repetition, in contrast to many other learning methods (Lakomy, 2019, p. 386).

In 2017, Disney's Maker Studios cut ties with the Swedish online gaming profile Felix Kjellberg, better known online as "PewDiePie", after reports emerged that he had made jokes containing anti-Semitic imagery or references, including a video in which the YouTuber paid two men to hold up a sign with the text "death to All Jews". The "PewDiePie" YouTube channel had 53 million subscribers at the time, making the channel one of the biggest in terms of audience reach (Winkler et al., 2017; Chokshi, 2017).

Gamification of violence

The use of video footage captured by HD cameras mounted on Da'esh fighters' helmets or the incorporation of gamified elements like points and rankings, both of which are typically associated with games and popular culture, have been used in propaganda and radicalisation efforts (Schlegel, 2020, p. 2).

On March 15, 2019, 28-year-old Brenton Tarrant entered the Al Noor Mosque in Christchurch, New Zealand, where he shot and killed 42 people. Exiting the mosque, he continued his killing spree, bringing the total death toll to 51 people. Tarrant was active on extreme right internet forums and approximately 10 to 20 minutes prior to the mosque being attacked, Tarrant visited the /pol/section of 8chan, an internet message board that is popular among the extreme right. Tarrant introduced himself in a post titled "*ahem*" as an anonymous user. "Well lads, it's time to stop shitposting and time to make a real-life effort post. I will carry out and [sic] attack against the invaders, and will even live stream the attack via Facebook." His 74-page manifesto, "The Great Replacement," which he used to justify the impending atrocity, was referenced in the link to his "writings", which led users to several file-sharing/storage sites. Tarrant had started filming himself using the Facebook Live app as he got in his car to head to his first target, as he had promised his fellow 8chan users. He turned to the audience and said, "Let's start this party" before entered the mosque wearing a helmet-mounted GoPro camera (Macklin, 2019, p. 18–19).

An essential and integrated part of Tarrant's attack was digital technology. Even more than his actual manifesto, his livestream served as the message rather than merely the means for it. According to Burke, the main goal of his attack was "to make a video of someone killing Muslims", rather than simply killing Muslims (Burke 2019 in Macklin, 2019, p. 19). Using a GoPro camera to capture the atrocity, Tarrant choreographed his assault to give it the appearance of a first-person shooter. Throughout his manifesto, Tarrant, made in-jokes about video games. He made fun of the fact that Spyro: Year of the Dragon "taught me ethnonationalism" and that Fortnite "trained me to be a killer" and "to floss on the corpses of my enemies." The "floss" is a dance move that Fortnite characters occasionally use. "Remember lads, subscribe to

PewDiePie," Tarrant advised viewers of his livestream before getting out of his car, referring to the well-known gaming YouTube channel (Macklin, 2019, p. 19–29).

Subsequent livestreamed terrorist attacks in Pittsburgh, El Paso, and Halle have included the use of gamified language and references to games, suggesting a "gamification" of violent extremism (Schlegel, 2020, s. 4). Gamification is the "use of game design elements within non-game contexts" (Deterding et al, 2011, p. 11). It entails introducing components like points, leaderboards, badges, or avatars into contexts that aren't typically thought of as play spaces with the goal of guiding user behaviour. Schlegel (2021a, p. 7) asserts that the Christchurch attack was the catalyst for gamification in the context of violent extremism and radicalisation to gain attention and resonate with target audiences. Currently, little is known about the ways in which gamification affects violent extremism. Even less is known about the potential benefits gamification could bring to P/CVE practitioners and their efforts to combat violent extremism.

The German-speaking Identitarian Movement's (IB) Patriot Peer app, which was planned but never released, is an example of top-down gamification. Top-down gamification is the deliberate application of game elements by extremist organisations or recruiters to promote interaction with their forums, platforms, and propagandistic content (Schlegel, 2021a, p. 6). Users of the Patriot Peer app were supposed to be able to compete with one another for the top spots on a virtual scoreboard by earning points for various activities, such as attending IB events or visiting designated cultural locations. Users could have discovered like-minded people using a Patriot Radar in a way similar to Pokémon-Go, giving the gamified application a social component (Schlegel, 2020, p. 17).

Bottom-up gamification refers to the naturally occurring emergence of gamified language and practices in lone individuals, small groups, and online subcultures without guidance from extremist organisations (Schlegel, 2021a, p. 6). This has been observed in numerous recent attacks, including those in El Paso, Halle, and Christchurch. For instance, users on 8chan commented on the high body count the attacker "achieved" after the attack in Christchurch and expressed a desire to "beat his score" (Schlegel, 2020, p. 15). Livestreaming is a method of gamifying the experience for both the perpetrator and the audience. The attack can be made into a game-like and "fun" activity by the perpetrator mirroring the livestreaming of well-known online games. For instance, the fact that the shooter in Halle, despite being a native German, conducted some of his livestream in English serves as an illustration of this according to Schlegel (2020, p. 15).

Data ownership

Video game player data refers to the way in which information about players' activities within a video game is stored and managed. This can include data such as game saves, achievements, high scores, purchases, decisions, and character customisation options. To ensure that games are engaging and challenging for players, the video game industry has traditionally invested heavily in marketing, advertising, and playtesting. To facilitate this, gaming companies often gather additional personal data from their customers. Today's shift to online, mobile, F2P and games-as-a-service has further enabled game developers and publishers to gather and process enormous amounts of information about players, including information about their online reading habits, gaming partners, and what motivates them to make purchases (Foust & Jerome, 2021).

Companies acquire player data through three primary methods: direct receipt from users during account creation or surveys, automatic extraction during interaction with their products (including games, digital stores, and websites), and data acquisition from third-party sources, including social media platforms. To access gaming services, it is often necessary to provide personal information such as name, email address, mailing address, and date of birth. Additionally, payment information may be required and stored for in-game transactions. Companies also gather geographical data about their players to provide the nearest server and match the player with others in similar time zones for optimal gaming experience (Bernevega & Gekker, 2022, p. 57). Methods to gather players data utilise hardware such as cameras, sensors, and microphones, as well as platform features such as linked social media accounts. Tracking technologies such as cookies are also employed. Moreover, geolocation data and biometric data, such as facial, voice, heart rate, weight, skin response, and eye-tracking data, can be collected during gaming sessions (Russel et al., 2018, p. 17).

In 2021, the leading gaming company in China, Tencent, introduced a facial recognition system in order to comply with China's efforts to tackle the issue of video game addiction among minors. Under the initiative, individuals under 18 years were prohibited from playing video games between 10 p.m. and 8 a.m. (Greig, 2021). The move sparked concerns regarding the state's use of biometric data to monitor its citizens, particularly as it encroaches on the privacy of minors. Tencent is not the only video game company to employ such measures, and the phenomenon of installing surveillance and control networks in video games is widespread (Egliston, 2022). In 2019, a database used by the Chinese Police was found to contain more than 300 million user messages sent through Tencent platforms and games (Denton, 2022). Additionally, each record included details on the type of device being used, photos, addresses, GPS location information, and ID numbers that could be used to personally identify Chinese citizens (Liao, 2019).

As players often engage with the game over extended periods of time, sometimes years, the game system can capture a plethora of information, ranging from actions taken on the platforms and within games to communication with other players (Kröger et al., 2021, p. 2). These player metrics are occasionally shared with users to enhance their gaming experience and

promote community building. In some cases, this is achieved through in-depth statistics of player performance. However, metrics are mostly employed to optimise game design and technology, inform business decisions, and enhance player experience (Bernevega & Gekker, 2022, p. 54). As such, the potential benefits of player data mining for both players and developers are enormous. However, the transition to games-as-a-service also necessitates that users have confidence in game designers to consistently uphold their right to privacy (Newman et al., 2014, p. 2). There are many examples in which players data has been compromised. One noteworthy instance of a data breach was the 2019 data breach at the game developer Zynga, where hackers were able to obtain the login details of individuals who played *Draw Something* and *Words With Friends*. The breach impacted 172 million accounts, making it one of the most substantial data breaches in gaming history (Ikeda, 2019).

In February 2023, the Ukrainian minister of Digital Transformation officially requested that Sony, Microsoft, and Valve to ban the sale of *Atomic Heart*, a video game which prominently incorporates Soviet Union, KGB, and Russian military elements. "I do believe neither of these businesses support bloody regime, murders or romanticizing communism. Brand new level of Russian digital propaganda – using gaming industry", he wrote in his tweet[18] linking the letter sent to the companies. The game, according to the minister, was developed by the Russian studio Mundfish. "As Mundfish has Russian management and offices, there is a potential risk that money raised from the purchase of the game will be transferred to Russia's budget, so it will be used to fund war against Ukraine," the letters stated.

One of the most common strategies for generating profit in F2P games is by matching users to advertisements. The main concerns with targeted advertisement in video games regards player privacy and the collection of data, who accesses it, how data is protected, and how it is being used. Moreover, as the data collected from players can be leveraged to gain insights into their psychological traits and cognitive vulnerabilities, such information can be utilised to create highly personalised advertising. The end goal for these advertisements may, in addition to marketing goods and services, be used to affect political opinions and beliefs (Kröger et al 2021., p. 2). For example, in 2018 it was discovered that the data analytics firm Cambridge Analytica, by gathering information from the Facebook accounts of about 87 million users, created psychographically targeted advertisements that sought to sway people's voting decisions in the 2016 US presidential election. The data was obtained, by others, through third-party "personality tests" and popular Facebook games such as FarmVille (Thulin, 2018). In this case the social media companies and advertising brokers, rather than gaming platforms, bore the brunt of the criticism, even though games were an important method for the breach.

[18] https://twitter.com/FedorovMykhailo/status/

Localisation & censorship

The process of adapting a video game for release in a different region or market is known as localisation. Localisation involves not just the translation of the game's text and dialogue into different languages, but also the modification of the game to fit cultural and regional preferences, as well as the adaptation of the game's marketing and promotion to the local audience. It requires the localisation team to have a deep understanding of both the source material and the target culture, as well as the technical skills to implement the necessary changes to the game. The localisation process is essential for game developers and publishers who want to reach a wider audience, as it allows them to tailor their games to the specific needs and preferences of different markets (Foust, 2022).

China is the world's largest video game market. As of 2021, Chinese gamers numbered around 740 million and more than $45 billion was spent annually on its domestic market (Holmes, 2021). Any international gaming companies wishing to do business in China are required by law to do so with a local partner. In 2011, Tencent and the American game developer Riot Games reached one of the first and largest agreements where Riot sold Tencent a 93 percent stake for an estimated $400 million. It sold the remaining equity four years later, becoming a wholly owned subsidiary of Tencent (Holmes, 2021). The following year, one of the biggest changes in PC gaming over the past ten years was brought about by Tencent's $330 million investment in Epic Games, the developer of, among others, *Fortnite*. This investment ushered in a new era of F2P. Since then, Tencent has seen a consistent increase in its annual revenue from online games and has maintained its position as the top game publisher in the world, dominating the market with a total revenue of $27 billion from their games business in 2021 (Batchelor, 2022).

Localisation also opens the door for censorship and information influence. The National Press and Publication Administration in China, which oversees censorship, has some very specific rules, such as not violating anyone else's copyright or disclosing state secrets. Media that promote cults and feudal superstitions are also prohibited, as are works that endanger social morality or national cultural traditions. Most of its regulations, however, are less detailed. Because of this ambiguity, censors have virtually unrestricted discretion in determining what is and isn't permitted (Holmes, 2021).

Since the market for video games in China is so large, aspects of Chinese censorship are frequently included during game development rather than removed before release (Foust, 2022). Self-censorship in video games refers to the practice of developers, publishers, or other industry stakeholders choosing to censor or restrict certain content in their games to avoid controversy or negative backlash. This can include a range of content such as violence, sexual themes, political themes, and more. Self-censorship in video games can be motivated by a variety of factors, including concerns about potential negative impact on players, fears of government censorship or regulation, and concerns about damaging the reputation or financial success of the game. While self-censorship can be a way for game developers and publishers to mitigate risk and avoid controversy, it can also be a source of controversy in itself. Some critics argue that self-censorship can have a

chilling effect on creativity and freedom of expression in the game industry and can lead to a homogenisation of content that fails to challenge or push boundaries. Others argue that self-censorship is necessary to avoid causing harm or offense to players or to society at large. Overall, self-censorship in video games is a complex issue that raises questions about the role of the industry in shaping cultural norms and values, and the balance between creative freedom and social responsibility on the one hand, and the power of states to censor on the other.

As of 2020, Tencent had over 300 investments in its portfolio (Messner, 2020). Numerous popular games, including *Player Unknown's Battlegrounds, Honor of Kings, Cross Fire,* and others, are owned by Tencent. These investments give Tencent the authority to impose Chinese speech norms on non-Chinese players at locations outside of China (Foust, 2022). China's second largest video game provider, NetEase, partnered with the US game developer Blizzard in 2008 to operate the Chinese versions of their games, including *Overwatch, World of Warcraft,* the *StarCraft* series, *Warcraft,* and *Heartstone* (Reynolds, 2022). After expressing support for the pro-democracy movement in Hong Kong, the top professional gamer Chung Ng Wai, known as Blitzchung, was kicked out of an international e-sports competition and had his winnings revoked in 2019 by Blizzard. In response to a question about whether Blizzard's partnership with NetEase had an impact on the decision, company president J Allen Brack said: "Was NetEase in conversation around this issue? They were, certainly." (Holmes, 2021). Blizzard's decision met with enormous criticism, and the company apologised and acknowledged that it "moved too quickly." The one-year suspension was shortened to six months and the prize money was returned (ibid). In November 2022, Blizzard announced that it would end its license with NetEase as

> *"The two parties have not reached a deal to renew the agreements that is consistent with Blizzard's operating principles and commitments to players and employees,"*
>
> (Reynolds, 2022)

Video game censorship is not exclusive to China. For instance, the Russian government announced in 2021 that it would censor video games released in Russia by using neural networks to look for and remove content that was illegal. The Russian government insisted that the censorship is necessary to highlight child sexual abuse in the media, suicide, and drug use, but the censorship, according to Foust (2022) goes far beyond these issues. This is nothing new. Previous examples of Russian attempts to censor video games include *Call of Duty: Modern Warfare 2* (due to the infamous "No Russian" mission, in which Russian terrorists indiscriminately murder civilians in a Moscow airport), *Company of Heroes 2* (due to its less-than-heroic representation of Russian forces), and other games that have sparked concern over play, such as *Pokémon Go* (due to fears it was being used by the CIA to gather video footage of the inside of Russian government facilities) (MacDonald, 2016).

Other examples of video game censorship include the 2020 Indian

government's decision to ban several Chinese owned video games, including the popular PlayerUnknown's Battleground Mobile (PUGB Mobile), allowing it to be reintroduced only after significant gameplay and content changes (EarlyGame, 2020a; 2020b), as well as the Medal of Honor: Warfighter and Call of Duty: Black Ops 2 ban in Pakistan. The ban was explained by the argument that the games "have been developed against the country's national unity and sanctity" (Conditt, 2013). According to Foust (2022), monitoring censorship on a global scale is complicated as many game developers do not want to come under scrutiny from governments in order to gain market access. In addition, there is at present no practical method for monitoring the influence of self-censorship by game developers.

Hacking, leaks & phishing

The black market around video games can refer to various illegal or illicit activities, including the distribution of pirated copies of games, the purchase of accounts from stolen or hacked games, and the purchase of cheats or game hacks. These actions have a variety of detrimental effects on players as well as the video game industry as a whole. One area where the black market around video games is particularly relevant to cybersecurity is in the sale of stolen or hacked game accounts. These accounts, which may contain valuable virtual items or in-game currency, can be stolen through a variety of methods, including phishing attacks and malware. In many cases cyber-criminals can purchase tools capable of illicit activities for a very low cost on dedicated hacker forums. Attackers frequently concentrate their efforts on games and game series that either have a large audience or were just recently released. *Valorant, Roblox, FIFA, Minecraft,* and *Far Cry* were among the top 5 games that cybercriminals used as a lure to spread secret-stealing software between July 2021 and June 2022 (Kaspersky, 2022). Threat data from the Kaspersky Security Network (KSN), a system for processing anonymous cyberthreat-related data shared voluntarily, showed that 384,224 users encountered gaming-related malware and unwanted software between July 2021 and June 2022. In the process of trying to download a desired game for free, find a cool mod, or find a cheat, players may end up with malicious software that can access their accounts, money, and sensitive data. Kaspersky found an increase in the number of attacks involving malicious software that steals private information from infected devices. This includes password-stealing tool Trojan-PSW, payment information stealing tool Trojan-Banker, and Trojan-GameThief which gathers login credentials for gaming accounts (Kaspersky, 2022). Once stolen, the accounts can be sold on the black market to other players, often at a significant markup. Account holders may lose access to their accounts and any virtual items or in-game currency that they have acquired, while game developers suffer an associated loss of revenue.

In 2011 and 2012, a 21-year-old hacker from Queensland, Australia gained access to Riot Games' European and North American servers, claiming to have accessed 24.5 million accounts along with encrypted credit and debit card numbers. The hacker's home was raided by the Australian Cybercrime Unit in March 2014, and his computer hardware was confiscated (Lewis, 2014). In 2022, Riot Games, home to several popular games such as *Grand Theft Auto,*

Max Payne and *Red Dead Redemption,* revealed in a statement on Twitter that it had "… suffered a network intrusion in which an unauthorised third party illegally accessed and downloaded confidential information from our system, including early development footage from the next Grand Theft Auto"[19 20]. In February 2023, TechCrunch reported that the popular game, *Call of Duty: Black Ops III*, had significant vulnerabilities that allowed hackers to take over players' computers if they were in the same online game. This caused some streamers to urge people not to play the game[21]. According to one online streamer on YouTube, hackers "… can join your game, they can kick you from the game, they can corrupt your [Downloadable Content], they can crash your game, they can fucking do anything they want,"[22] (Franceschi-Bicchierai 2023c).

In April 2023, an investigation was launched by the US Justice Department and Pentagon after a number of top-secret documents were leaked on a Discord channel related to the Minecraft computer game, before they spread to other sites such as 4Chan, Telegram, Twitter, and major media publishers around the world. These documents included, among other things, intelligence related to Russia's invasion of Ukraine (Toler, 2023). The leaker was allegedly a member of the National Guard who shared the documents with a small international community in order to keep them informed about current affairs[23]. Some have suggested that the documents included so-called tainted leaks, in which critical information has been deliberately altered to mislead readers[24].

The leak of sensitive military documents on gaming related platforms is not entirely unprecedented, although unusual. In 2019, prior to the UK general election, a similar leak occurred in which documents relating to UK-US trade relations was released on gaming-related forums on platforms such as Reddit and 4Chan. Reddit later confirmed that the documents had originated from Russia (Adams, 2023). Similarly, since 2021 there have been three separate incidents where players of the popular video game *War Thunder* have posted classified documents about tanks of British, French, and Chinese origin in an online forum dedicated to the game. One player uploaded a classified manual for the British Challenger 2 tank claiming that they did so in the hopes of getting a *War Thunder* developer to improve the accuracy of the tank in the game. Another user who claimed to be part of a French tank unit uploaded a Leclerc S2 manual while engaging in a discussion about its turret rotation speed (Smith, 2022).

In March 2023, GSC Game World, the Ukrainian company developing *STALKER 2*, claimed that hackers had obtained game data and were blackmailing them. An anonymous user on VKontakte, a Russian social media platform, claimed to have carried out the breach and threatened to leak game data unless the developer agreed to a series of demands. These demands did not

[19] https://twitter.com/RockstarGames/status/
[20] https://www.youtube.com/watch?v=aDkCu1MVWPM
[21] https://www.youtube.com/watch?v=k12zZ8bMlYg&feature=youtu.be
[22] https://www.youtube.com/watch?v=k12zZ8bMlYg
[23] https://www.dailymail.co.uk/news/article-11967397/Leaker-posted-secret-Pentagon-documents-works-military-base-20s.html
[24] https://www.bbc.com/news/world-europe-65225985

include payment, but rather inclusion of Russian-language localisation, including voice acting and place names, an apology to Russian and Belarusian players, and the unbanning of a Discord account.[25]

Phishing refers to the use of fraudulent emails or websites to trick individuals into divulging sensitive information, such as login credentials or financial information. It is a type of online fraud in which scammers try to get access to personal information by posing as a reliable source (Porter, 2021). In the context of video games, gamers can for example receive emails from scammers asking them to verify their passwords and login details. A fake sign-in page that requests a user's current password and username will be displayed to gamers who click the link in the email. Once users provide these details, scammers can access their accounts and take control of their virtual credits, or money stored in the users' online wallets. The accounts that were compromised as well as the virtual currency may then be auctioned on the dark web (Rafter, 2020). Kaspersky found over 3.1 million attacks related to phishing activities in online games between July 2021 and June 2022 (Kaspersky, 2022). A common technique is to offer quick in-game currency. For instance, there have been numerous instances where fake websites akin to the Grand Theft Auto Online website ask users to login to access in-game features. Once the login details are disclosed, the cybercriminals have access to private data like gaming accounts, phone numbers, and even banking information. Similar fake marketplaces have been established under the names of the well-known e-sports games PUBG, Warface, and CS:GO (Kaspersky, 2022).

In December 2022, Activision was subjected to a SMS phishing attack that they claim was unsuccessful (Franceschi-Bicchierai 2023a). However, in February 2023, the cybersecurity and malware research group vx-underground published screenshots demonstrating that the phishing attack had in fact been successful. According to vx-underground, "they exfiltrated sensitive work place documents as well as scheduled to be released content dating to November 17th, 2023".[26] This was later confirmed by Insider Gaming, stating that they had "been able to verify the legitimacy of the alleged Activision data breach from Twitter user @ vxunderground". According to Inside Gaming, the data obtained in the hack included "plans for Modern Warfare 2's upcoming DLC's, Call of Duty 2023 (Codenamed Jupiter), and Call of Duty 2024 (Codenamed Cerberus), as well as sensitive employee information" (Henderson, 2023).

Similarly, Reddit, a social media platform home to a large video game community, suffered a sophisticated phishing campaign targeting its employees in February 2023. In an official statement[27], the company revealed that the attacker used credible-looking prompts to lure employees to a fake intranet gateway website, aiming to steal their credentials and second-factor tokens. According to the statement, there was no indication of any compromise of Reddit's primary production systems that store the majority

[25] https://www.polygon.com/23637543/stalker-2-hack-russian-war-in-ukraine-threats
[26] https://twitter.com/vxunderground/status/1627477748359872513
[27] https://www.reddit.com/r/redditsecurity/comments/10y44g0/we_had_a_security_incident_heres_what_we_know/

of data and run the platform. The exposure was limited to the contact information of hundreds of current and former employees and advertisers. In 2018, Reddit encountered a severe data breach that resulted in attackers gaining access to an entire copy of Reddit's data from the first two years of the platform's operation. The data compromised included usernames, hashed passwords, emails, public posts, and private messages (Page, 2023).

Another example of phishing includes a massive phishing campaign carried out throughout 2022 by the hacking group oktapus. According to the cybersecurity firm Group-IB's analysis, over 130 organisations were victims of the sophisticated attack using simple phishing kits. The attackers aimed at employees working for companies that utilise the services of the leading IAM provider, Okta. The said employees were sent text messages that included links to phishing sites, which imitated their organisation's Okta authentication page. At the onset, the attackers had a clear objective in mind – to acquire the Okta identity credentials and two-factor authentication (2FA) codes of the targeted organisations' users. This would enable them to illicitly access any enterprise resources that the victims have permission to use (Mirkasymov & Martinez, 2022). Among the targeted companies were a few prominent game makers, such as Riot Games and Epic Games (Franceschi-Bicchierai, 2022a).

Anti-cheat & DRM

DRM (digital rights management) refers to the technologies and practices that are used to protect digital content from unauthorised use or distribution. DRM-cracking is the practice of bypassing or circumventing DRM measures, which may be done to pirate or distribute unauthorised copies of games. Publishers use DRM in most modern games to thwart cheating and piracy (Roach, 2020). Kaspersky found 3,154 different files distributed as cheat programs for the most popular game titles between July 1, 2021, and June 30, 2022. The majority of the files imitating cheat software were connected to *Total War, Roblox, Valorant,* and *Counter-Strike: Global Offensive* (Kaspersky, 2022).

Anti-cheat measures are techniques or technologies that are used to prevent players from using unauthorised cheats or hacks in games. These measures can include software that detects and blocks the use of cheats, as well as systems that monitor players' actions and flag suspicious behaviour. Anti-cheat software frequently starts a signature-based scanner to look for potential cheats and weaknesses in the memory and running processes of a computer. An incident report is sent to the gaming company's engineers for analysis if the scan turns up any anomalies. If the engineers find a match between the cheat and their database, they will flag the account, and any additional cheats will be added for future investigations. Concerns about the software designed to find and eliminate cheaters have increased among some gamers, who believe it now poses a severe threat to their privacy and the integrity of the system (Menegus, 2022). For example, in 2014, Valve's Anti-Cheat was accused of prying into players' web browsing habits, "reading all the domains you have visited", and sending it "back [to Valve's servers] in hashed form" (Boyd, 2014).

Kernel-level drivers, also known as "ring 0," are compartmented area of a computer where its essential operations are carried out. The operating system, hardware drivers (such as those for keyboards, mice, and video cards), and software that needs high-level permissions (such as antivirus programs) are all included in this category of software (Menegus, 2022). In 2013, an ESEA developer converted computers into a bitcoin mining farm using the software's kernel access. Before being discovered, the developer made nearly $4,000 by using the GPUs of unaware players (Conditt, 2020). While faulty code running in "ring 3," where browsers, and the rest of the software resides can cause that particular software to crash, faulty code running in the kernel compromises the entire system (Menegus, 2022). Attackers can alter game memory from ring 0, bring down the system, or access files belonging to other users (Conditt, 2020).

In 2020, Riot Games' first-person shooter game *Valorant's* always-on-anti-cheat system Vanguard raised legitimate privacy concerns. Weeks after *Valorant* and Vanguard launched in 2020, Reddit was flooded with complaints and conspiracies about Vanguards gathering of player data. While other well-known kernel-level anti-cheat programs, like *Fortnite's* Easy Anti-Cheat and *DayZ's* BattlEye, also use kernel drivers, they only function when the game is running. Vanguard, on the other hand, consists of two main parts: a device driver that loads at system startup and a traditional scanning service that starts when the game does. That means that even when not playing Valorant, the driver keeps running the entire time the computer is on (Conditt, 2020).

More recently, Riot Game revealed that hackers had succeed in obtaining the source code for its most popular games *League of Legends* and *Teamfight Tactics*. In addition, the hackers got hold of the source code for their legacy anti-cheat system, which may result in hackers developing more evolved and harder-to-detect exploits (Francheshi-Bicchierai, 2023b). In a tweet, Riot Games stated that "any exposure of source code can increase the likelihood of new cheats emerging,".[28] According to the company, the attack did not compromise any player data or personal information.[29]

Mods

The term "mods," which is short for "modifications," describes user-made changes or additions to games. Mods can include small changes to game-play mechanics or substantial rewrites of the game's narrative. While some mods might be created and distributed legally, others can be made and distributed without the game developers' consent. Early in the 1980s. *Castle Wolfenstein* (1981) was completely remade as *Castle Smurfenstein* (1983), that not only swapped Nazis for Smurfs but also altered the text, graphics, and audio of the game. This is typically regarded as the first mod. Since then, there has been a complicated and contentious relationship between modders and the industry. Companies' strategies for dealing with modding range from allowing users to create and sell mods, providing official tools for creating

[28] https://twitter.com/riotgames/status/1617900237431111683
[29] https://twitter.com/riotgames/status/1616548651823935488

mods, to enforcing legal action to outlaw the creation and distribution of some or all mods (Kretzchmar & Stanfill 2019, p. 521).

In 2022, Roblox, the world's biggest gaming platform for children, removed two mods in which players fought and killed each other either as Russians or Ukrainians. The games, *War on Larkiv: Ukraine and Battle for Ukraine,* were based on the ongoing Russian invasion of Ukraine and allowed players to watch and participate in the bombing of cities such as Mariupol. The game page of *War on Larkiv: Ukraine* read "Grab your guns and choose your side of the fight in the *War of Larkiv: Ukraine*. Heavy combat is taking place right now in the fictional city of Larkiv, soldiers strive with hope and destiny". The game became very popular with a review score of 71% from users, with over 90,000 plays in less than two weeks. The game also gained a large audience on TikTok, with 4.7 million views on videos posted with the title (Tidy, 2022). Ukraine War Mod is another mod stimulation the war. It is a free mod for the popular FPS *Battlefield 2* where the original setting, a fictional war between the United States and China, is changed to Ukraine and Russia. The mod allows players to take the role of Ukrainian troops. "For *Battlefield 2* players looking to act out the Russian invasion of Ukraine, this mod provides a way to do that," Softonic states in their review[30] of the mod. Additionally, there are strategic simulation game mods that allows players to rule the United States as Donald Trump (Gualt, 2016). Other examples include a mod that replaces Skyrim's banner with the Ukrainian flag in *The Elder Scrolls V: Skyrim*.[31]

As previously mentioned, footage from video games such as *Arma 3* and *Digital Simulator World* have been used in ongoing conflicts claiming to show real-world footage. As these games have active mod community with skilled users, there is a risk of mods based on real-life events being used to misleading people into believing that the footage shown is real (Coontz, 2022).
Prior to the 2020 US presidential election, the media platform for modding PC games, NexusMods, announced[32] an outright ban on political troll mods in games.

> *"Recently we have seen a spate of provocative and troll mods being uploaded based around current sociopolitical issues in the United States. As we get closer to the US election in November we expect this trend to increase as it did this time 4 years ago," the statement read.*

The statement advised users not to engage with such mods and to report them. The decision was described as due to poor quality of the mods, their divisive views, and "the fact that a small but vocal contingent of our users are seemingly not intelligent or grown up enough to be able to debate the issues without resorting to name calling and baseless accusations without proof." Political themed mods are not new, but rather a recurring theme. For instance, in Grand Theft Auto V, players can modify the textures of semi-truck trailers to display messages supportive of Ben Shapiro and Donald Trump.[33]

[30] https://ukraine-war-mod.en.softonic.com/
[31] https://www.nexusmods.com/skyrim/mods/112915
[32] https://www.nexusmods.com/news/14373
[33] https://www.nexusmods.com/gta5/mods/221

Money laundering

In-game currency is a common feature in video games, allowing players to purchase virtual goods or upgrade their characters using real-world money. Although this feature is popular amongst gamers, it has also created a potential loophole for illegal activities such as money laundering. This has been observed in popular games like *Fortnite* and *World of Warcraft,* as well as free-to-play games that offer in-game currency for purchase with real money (Belding, 2021). There are two types of virtual currencies: convertible and non-convertible. While non-convertible currencies can only be used for in-game purchases, convertible currencies can be exchanged for real money. Crypto-currencies, such as Bitcoin and Ether, are examples of convertible virtual currencies that are protected by cryptography and recorded on a secure, decentralised ledger (Kelly, 2021, p. 1495). The exchange of virtual goods for real currency is a key feature that enables money laundering through online games. The value of in-game items in the virtual world can translate into real-life value outside the game, providing a means for criminals to conceal their illicit proceeds (Moiseienko & Isenman, 2019).

Online video games have been a suspected avenue for money laundering for decades. In 2005, it was estimated that eBay was trading approximately $30 million worth of in-game goods per year (Castronova, 2005, p. 149). According to TrendLabs (2019, p. 9), gaming currency is often acquired through exploiting bugs and stealing game credentials with the help of malware. Criminals resell the stolen currency through websites and social media to convert payments into cryptocurrency and make them untraceable, which is used to fund other criminal operations.

In 2019, Valve suspended the trading of some in-game items for the popular game *Counter Strike* after discovering that most of this trading was part of a global money-laundering scheme. "At this point, nearly all key purchases that end up being traded or sold on the marketplace are believed to be fraud-sourced", Valve said in an official statement (Valve, 2019). Valve's announcement underscores the vulnerability of online gaming marketplaces to fraudulent activities.

The online gaming industry has relatively lax regulations compared to other online transactions. The transfer of in-game currency is simple, and congested gaming platforms can provide cover for criminals to hide their transactions, making it easier for illegal activities like money laundering to take place (Cotter, 2022). For instance, an investigation by The Independent and the cybersecurity firm Sixgill found that criminals use stolen credit card details on online black markets to purchase V-bucks, the virtual currency used to buy items in Fortnite's official store, and sell it to players at a discounted rate, effectively laundering the stolen money (Cuthbertson, 2019). Similarly, in 2018, it was discovered that a group of cyber criminals had utilised stolen card information to create multiple Apple IDs and purchase in-game items in mobile games like *Clash of Clans* and *Marvel Contest of Champions*. These items were then resold on third-party websites for real money (Lishchuk, 2021).

In addition to video games functioning as a means for money laundering, the structure of online video games and associated social platforms enables

extremist and terrorist groups to raise money. Donations as a means for funding terrorism and extremism are not new (Squire, 2021, p. 1). However, the development of online content subscriptions and livestreaming platforms has increased access to these services and, consequently, the opportunity for illicit groups to raise money using funding methods associated with video games. For example, a study by the Institute for Strategic Dialogue (2020) describes the potential for fundraising offered by donation-only websites like Patreon and Subscribestar as well as content delivery services like DLive. They found that 14 far-right groups and three hate groups were using these services to raise money. In a study on the economics of streaming ecosystems, Squire (2021) discovered that far-right actors can raise more than $100,000 in donations in under a year with a regularly produced live-streams on DLive.

Several voluntary measures have been implemented by mainstream social media companies such as Facebook, Google, and Microsoft to identify and remove terrorist and extremist content to prevent them from taking advantage of their platforms to spread propaganda. Similarly, the decentralised cryptocurrency computing platform Ethereum is covered by the fifth Anti-Money Laundering directive as a means to prevent the cryptocurrency being used by terrorists and extremists (EU Counter-Terrorism Coordinator, 2020, p. 3). Gaming platforms, however, are not subject to the same levels of regulation as mainstream social media platforms or cryptocurrencies. They consequently function in a sort of vacuum and are therefore vulnerable to abuse by terrorists and other criminals (ibid).

4| Platform-specific vulnerabilities

4. Platform-specific vulnerabilities

In this chapter, the main video game platforms for live streaming, distribution, subscription services, collaboration, and communication between gamers are introduced. The chapter focuses on how they have been exploited by malign actors and which measures the platforms have taken to combat extremism, disinformation and harmful content. This is obviously something that is work in progress and may change quickly dependent on developments, so the information provided here is primarily about establishing a basis for further analysis. The platforms that are described below are: Discord, DLive, Nintendo Switch Online, PlayStation Network, Steam, Twitch, Xbox Network, and YouTube. Note that some platforms are primarily or solely for gaming-related activities, whereas others provide a broader set of services.

Discord

Discord was originally founded in 2015 with the aim of providing gamers with an effective communication tool while collaborating on multiplayer games. The platform offers real-time voice, text, or video chat, as well as the ability to exchange music, videos, and files (EU Counter-Terrorism Coordinator, 2020). Users can create public or private servers to connect with other gamers who share their interests, utilizing features such as forums, chat, and audio and video communication. Discord currently has nearly 7 million servers, over 300 million registered accounts, and over 140 million active users each month (Schlegel, 2021b, p. 4).

Researchers have noted that extremist groups use Discord due to an architecture that allows the creation of "tight communities." (Guhl et al., 2020, p. 9). These groups serve two primary purposes: to create a secure environment for young people interested in extremist ideologies to connect and learn, and to coordinate online harassment of minority groups (Davey, 2021, p. 8). A study by ISD found that racist trolls and neo-Nazi content are present on Discord servers, drawing from the white nationalist and white supremacist forum culture of 4chan and 8kun. Neo-Nazi content is also present on these servers (ibid, p. 6). Furthermore, Discord's extreme right channels are frequented by very young people, raising concerns that the platform is being used to radicalise young people. The average age for users in the sample used by ISD was 15 (ibid, p. 7). Discord has also been used to organise offline gatherings, such as the Unite the Right rally in Charlottesville, Virginia, in August 2017. Discord was utilised in this case by the event's organisers for both planning and promotion of the gathering as well as for

the dissemination of propaganda and far-right violent extremist rhetoric, such as praising Hitler within servers for outwardly violent extremists (such as "Führer's Gas Chamber") (Gallagher et al., 2021, p. 4).

To combat extremism and harmful content on its platform, Discord has implemented policies that prohibit the organisation, promotion, or support of violent extremism. Discord stands out in the gaming industry for its inclusion of the term "extremism" in its policies, which prohibit the organisation, promotion, or support of violent extremism (Lakhani, 2021, p. 17). Violations of this policy result in warnings or immediate account termination, depending on the severity of the offense. For issues like violent extremism or child sexual abuse material they immediately disable the account and remove the offending content (Discord, 2022). The platform recently acquired Sentropy, "an AI-based software company focused on fighting abuse and harassment online," and Discord has expanded its policy team. The policy team works with consultants to audit their hate speech policy, to identify gaps, and look for potential improvements. Additionally, Discord has ties with groups like The Global Internet Forum to Counter Terrorism (GIFCT) in an effort to form closer industry partnerships (Lakhani, 2021, p. 17).

A policy prohibiting harmful misinformation was added to Discord's Community Guidelines in February 2022. The updated policy stated that "users may not share false or misleading information on Discord that is likely to cause physical or societal harm". Moreover, users were from now on encouraged to report harmful misinformation to Discords Trust & Safety team (Anderson, 2022).

In April 2023, Brad Smith, the president of Microsoft, claimed that the Russian intelligence agencies and The Wagner Group have been attempting to infiltrate gaming communities. Responding to a leak of top-secret Pentagon documents about the Ukraine war that were believed to have originated from Discord, Smith revealed that Microsoft's threat analysis team had been identifying the Russian attempts to infiltrate gaming communities. Discord given as an example by Smith. Gaming communities, he said, "just happen to be a good place for them to get the information into circulation, and then ultimately journalists find it."[34]

DLive

DLive is a livestreaming platform that was founded in 2017 and acquired by BitTorrent in 2019. As of 2020, DLive had 5 million monthly active users (Mahmoud, 2022, p. 65). According to its website, DLive's goal is to develop a value-sharing live streaming platform that, through an innovative rewards program, empowers both creators and viewers (DLive Community, 2021).

Like Twitch and YouTube, DLive is a video streaming service that enables users (also known as "streamers," or "content creators") to record themselves talking, playing video games, and other activities. Other users can watch this content in real-time and engage with it by texting or making a monetary donation (Squire, 2021, p. 1). DLive offers a feature akin to YouTube's "Super Chat," where viewers can pay to communicate with content producers directly during a live stream, and the website will then post whatever they

[34] https://twitter.com/semafor/status/

write (Gais & Edison Hayden, 2020).

DLive is built on blockchain technology, using its own currency directly through it rather than relying on advertising revenue. Blockchain is a secure data storage technique that employs a decentralised network of peer-to-peer nodes to store public transactional records, which are also known as "blocks." The blockchain technology framework ensures that the data is resistant to manipulation, hacking, or unauthorised changes. This type of storage is frequently referred to as a "digital ledger." Every transaction in this ledger is validated and protected against fraud by the owner's digital signature, which also serves to authenticate the transaction. As a result, the data in the digital ledger is very secure (Cohen, 2020). The "lemons" that represent credits are earned on DLive over time by watching livestreams broadcast on DLive, with each lemon having a value of $0.012. The lemons, which are typically accumulated by users transferring funds to their own accounts, can then be converted into cash donations by DLive account holders (Gais & Edison Hayden, 2020).

DLive charges a 25% fee on all platform transactions as opposed to traditional platforms' 50% fee (DLive Community, 2021), thereby potentially making the platform more profitable than tools like YouTube's Super Chat (Gais & Edison Hayden, 2020).

The emergence of blockchain technology has also created opportunities for reduced censorship. Due to the decentralised nature of blockchain platforms, content deletion from numerous servers takes longer than centralised systems. While DLive has community guidelines that forbid harassment or hate speech, it also allegedly provides users with protection from deplatforming, a practice where tech companies prevent individuals or groups from using their websites (Cohen, 2020). DLive's lack of content moderation and deplatforming has attracted far-right extremists and fringe streamers who have been barred from mainstream social media platforms like YouTube (Cohen, 2020; Gais & Edison Hayden, 2020). PewDiePie, one of YouTube's most popular content creators with nearly 94 million subscribers, moved exclusively to DLive in 2019. Although financial factors played a significant role in PewDiePie's decision, some have been drawn to DLive as a consequence of being deplatformed from other video streaming services (Gais & Edison Hayden, 2020).

According to recent findings from ISD, extremist groups have taken advantage of the relative lack of content moderation. The platform has been used to spread racist, sexist, and homophobic content, as well as conspiracy theories that would likely be banned on other platforms (Thomas, 2021). DLive is also known to have played a role in the events leading up to the January 6th Capitol insurrection, with far-right extremists livestreaming the event and receiving donations from viewers (Lakhani, 2021, p. 9). In response to the storming of the Capitol, DLive has implemented stricter content moderation policies, including demonetisation and the banning of influential figures associated with far-right extremism (ibid, p. 18). The findings of ISD's analysis of DLive indicates that these actions reduced the "safe harbor" that extremists had previously enjoyed on DLive (Thomas, 2021). However, some claim that extremism still has a foothold on the platform despite these efforts to remove it (Schlegel, 2021b).

Nintendo Switch Online

Nintendo Switch Online is a digital subscription service provided by Nintendo for the Nintendo Switch gaming console. The service was launched in 2018 and is primarily designed to enable online multiplayer gaming, which allows players to participate in games with other players across the globe. Similar to many of its competitors, the service requires a subscription fee to access its services (Roach & Yade, 2022).

Apart from online multiplayer gaming, the Nintendo Switch Online also offers a diverse library of classic games from various gaming systems, including NES, N64, and Sega Genesis. Subscribers of the service can access these games for free with their subscription. The Nintendo Switch Online is required to access the online features of first-party Nintendo games and many third-party games. However, free-to-play games such as Fortnite and Rocket League can be accessed without a subscription. The Nintendo Switch Local Wireless Play feature allows multiplayer gaming between two Switch consoles, with up to three players on each console. For voice chat during online games, Nintendo provides a mobile app that is available for both iOS and Android devices (Nintendo, n.d.).

In January 2023, Modulate announced that its voice-moderation tool for games, ToxMod, was available on the Nintendo Developer Portal. This enables game developers creating games for the Nintendo Switch to be use ToxMod in their games (Conell, 2023). ToxMod uses machine learning to triage voice chat data and analyze the tone, context, and intention of conversations. It then escalates the most toxic chats to moderators, who can take action to mitigate bad behaviour (Modulate, n.d.). According to Modulate, "Proactive voice-native moderation identifies more than 30x the amount of toxicity than player reports alone". This is still, however, in the early stages of implementation.

PlayStation Network

Sony Interactive Entertainment offers PlayStation Network (PSN), an online entertainment platform that provides access to a wide range of features. Originally designed for PlayStation gaming consoles, PSN has expanded to include various other devices such as smartphones, tablets, high-definition televisions, and Blu-ray players. The service was launched in November 2006 and allows users to create an account that can store games and other multimedia content, making it a versatile platform for entertainment seekers. The accounts are created for free but services on the platform such as multiplayer gaming can only be accessed for a fee (Playstation, n.d.).

In 2011, approximately 77 million account holders' personal information was compromised, and users of PlayStation 3 and PlayStation Portable consoles were unable to access the service. The hack occurred due to an "illegal and unauthorised person" gaining access to Sony's PlayStation Network and Qriocity services (Quinn & Arthur, 2011). Sony took significant steps to improve data security and protect consumer information after the hack. This included working with external security firms to implement new security measures, adding advanced technologies and software monitoring,

penetration, and vulnerability testing, and increasing encryption and firewalls. Additionally, they introduced an early warning system for unusual activity to detect potential network compromises (Sony, 2011).

Although PSN has taken various measures to improve security, the platform has faced scrutiny for its potential misuse by terrorists. Following the terrorist attacks in Paris 2015, several news outlets suggested PlayStation 4's were used to plot the attacks, quoting the Belgian deputy prime minister saying that "The most difficult communication between these terrorists is via PlayStation 4," and that "It's very, very difficult for our services – not only Belgian services but international services – to decrypt the communication that is done via PlayStation 4." (Yin-Poole, 2015). The PlayStation 4 had a robust protection system that proved difficult for many advanced national security services to breach. This was due to the implementation of the Transport Layer Security (TLS) protocol, which employs symmetric encryption (AE256CBC) and 2048-bit asymmetric (RSA) encryption keys, making it one of the most sophisticated encryption systems worldwide (Sáfrán, 2022, p. 188). The statement was, however, part of a debate held three days prior to the attacks and no directs link between the attacks and PS4 has yet been made. After the remarks, Sony acknowledged that the PS4 could be misused, but emphasised that the communication functionalities of the console were similar to those of other internet-connected devices in common use (ibid).

A 2016 EU IRU analysis drew attention to the possibility of jihadi groups using gaming consoles like PlayStations and identified challenges in investigating terrorist communications on these devices, particularly with respect to the use of voice over IP (VOIP) technologies. Furthermore, the prevalence of guns and violence within these games makes it more difficult to automatically identify potential threats (EU Counter-Terrorism Coordinator, 2020, p. 8). The same year, The Counter Extremism Project (CEP), an anti-terrorism group founded by former US government officials, pressed Sony on the extent of terrorist communication on the PlayStation 4 network, asking Sony what steps it was taking to limit this activity. The letter to Sony cited a number of reports claiming that Da'esh uses PlayStation's network because it is strongly encrypted and hard to monitor (Nasr, 2016).

Despite these challenges, Sony has implemented various security measures to protect against unauthorised access and activity on the platform, including monitoring for unusual behaviour and implementing encryption and firewalls. Additionally, PSN has policies in place to prohibit users from engaging in illegal or harmful activities, and the company works with law enforcement to investigate and address any reported violations. For example, Sony provided information to the FBI in 2018 regarding a PlayStation 4 user who was suspected of planning to join Da'esh in the Middle East. The data contained the suspect's decrypted communication history, indicating that certain prominent gaming platforms' encryption protocols may allow collaboration between the platforms and law enforcement authorities in particular situations (EU Counter-Terrorism Coordinator, 2020, p. 8).

Steam

As the "ultimate destination for playing, discussing, and creating games", Steam was first introduced in 2003 and has become the largest distribution site for PC games (Vaux et al., 2021, p. 4). It currently has over 120 million monthly active users and 63.6 million daily active users as of 2021 and boasts over 50 million games in their online catalogue (Dean, 2021). Steam's popularity has also made it a target for cybercriminals, as evidenced by a significant data breach in 2011 in which hackers gained access to the platform's user database, stealing usernames, encrypted passwords, email addresses, and other sensitive information. The breach affected over 35 million users and was believed to have been caused by a vulnerability in the platform's forums (BBC News, 2011).

Money laundering has been observed on the platform. For instance, Valve revealed in 2018 that a significant portion of micro-transactions in the widely played game *Counter-Strike Global Offensive* were involved in money laundering activities (EU Counter-Terrorism Coordinator, 2020, p. 12). The primary area of controversy for Steam has been in content moderation. In 2017 and 2018, Vice (Maiberg, 2017), the Huffington Post (Campbell, 2018), and Reveal (Carless & Sankin, 2018) reported on Steam users and groups promoting content that was racist, sexist, homophobic, antisemitic, and otherwise hateful. This included Nazi imagery and groups glorifying school shooters. In response, Valve announced a new moderation policy for the platform in which they would "allow everything onto the Steam Store, except for things that we decide are illegal, or straight up trolling." The statement made it clear that offending someone shouldn't take away a game's voice, and that developers should be able to express themselves and find others who want to play their game (Steam, 2018a). According to the head of research and policy of far right and hate movements at ISD, while conducting research on Steam, they observed that several accounts on Discord, DLive, and Twitch were taken down during the course of the investigation. However, on Steam, those same accounts remained active, suggesting that Steam's moderation efforts against harmful activity are rather limited.

Despite the steps taken by Steam to improve its content moderation, concerns about the platform's lax approach to moderation persist. Some critics argue that the platform's "very loose set of content guidelines" makes it a breeding ground for hate speech, harassment, and other toxic behaviour (Bedingfield, 2021). Until 2018, discussion board content moderation was left up to the game developers' judgment. In September 2018, Valve announced that it would start moderating user-flagged content on Steam discussion boards for some particular games. Following the moderation update, when a player flags a forum post or discussion thread in the community, it is added to a queue for Steam's moderation team to review. Any posts that are reported as being in violation of Steam's Community Guidelines will be reviewed and removed (Steam, 2018b).

Since introducing this new policy, Valve has taken several related steps including a 2019 decision to not let the game Rape day be sold on Steam as "… this developer has chosen content matter and a way of representing it that makes it very difficult for us to help them do that" (Steam, 2019). The

decision was made due to "unknown costs and risks" to Valve, developer partners, and customers, and not due to the game's misogynistic and celebrated violence against women, according to the Anti-Defamation League (2020). Over 170 games have now been removed from the platform and in December 2019, Valve removed 50 instances of Nazi-related user content, in compliance with a request from the German government (ibid).

A recent study the Institute for Strategic Dialogue (ISD) found that Steam has an established and long-lasting extreme right community. The study found that Steam was primarily used to create and strengthen these communities, as well as to point users to off-platform content such as the official websites of extremist groups. These communities were discovered to have been present on Steam since at least 2016, with a network of violent extremists also present (Davey, 2021).

In conclusion, while Steam is a popular and valuable platform for gamers and game developers, it has a history of allowing extremist content and communities to thrive. While the company has taken some steps to moderate content, recent findings suggest that further action may be necessary to ensure that Steam is a safe and inclusive platform for all.

Twitch

Twitch, an Amazon-owned platform introduced in 2011, allows users to livestream themselves playing video games while others watch and engage with them through real-time chat features (Lakhani, 2021, p. 8). As of 2020, Twitch had 9.5 million active streamers (Mahmoud, 2022, p. 65).

In its first transparency report covering 2020, Twitch acknowledges that the platform's livestreaming nature requires various strategies to address safety-related issues. These strategies include machine learning, moderators, user reporting, partnerships, and more (Twitch, 2021). Due to the significant amount of extremist activity on the platform, Twitch updated its community guidelines and expanded its prohibition on material supporting terrorism and extremism. It also established an internal moderation team to prevent channels from breaking the rules (ibid). Furthermore, despite not being a top-down initiative, there is evidence of counter-speech content being used on Twitch to combat far-right (violent) extremism on the platform (Lakhani, 2021, p. 18).

According to Twitch's 2020 transparency report, "Content moderation solutions that work for uploaded, video-based services do not work, or work differently, on Twitch" (Twitch, 2021). The platform further developed this reasoning in its transparency report covering the first half of 2022 by stating that "safety cannot be one-size-fits-all" due to the varying needs of streamers and communities (Twitch, 2022a). Twitch updated its Community Guidelines in 2021, including the "Off-Service Conduct Policy" and a policy allowing the platform to preemptively suspend accounts when a user's use of Twitch poses a high likelihood of inciting violence in the real world (Twitch, 2022b).

In March 2022, Twitch implemented a new strategy for combatting harmful misinformation on its platform in collaboration with third-party experts, including the Global Disinformation Index. The platform stated that its goal was to prohibit individuals whose online presence is dedicated to spreading

harmful, false information from using Twitch (Twitch, 2022c). Twitch claims that it will act against actors who fit the criteria of persistently sharing widely disproven and broadly shared harmful misinformation topics, such as conspiracies that promote violence, both on and off the platform (ibid).

Xbox Network

Microsoft Corporation created Xbox Network (formerly branded as Xbox Live) in 2002, as an online gaming and entertainment platform primarily for the Xbox gaming console. The launch statement read, "With Xbox Live, players can connect with each other across the country, chatting with old friends and meeting new ones to share game experiences online, no matter where they are or what time of day it is" (Microsoft, 2002). Over the years, Xbox Network has extended its services to other devices such as personal computers, smartphones, and tablets, and as of January 2021, Microsoft announced that the number of users had surpassed 100 million (Warren, 2021).

Xbox Network provides its users with a wide range of digital services, including an online marketplace known as Xbox Store. It also offers a premium subscription service called Xbox Game Pass, which provides enhanced gaming and social features. The platform also has a cloud gaming service called Xbox Cloud Gaming (formerly known as Project xCloud) that allows subscribers to stream Xbox games on their smartphones or tablets (Hollister, 2020).

However, the Xbox Network has not been without its controversies. In 2013, leaked documents from former NSA contractor Edward Snowden claimed that the US National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) infiltrated gaming communities and built mass-collection capabilities against Xbox Live and other online gaming networks. The agencies viewed online gaming as a "target-rich communications network", where terrorists might lurk (Ball, 2013). According to the documents, NSA agents investigated the potential use of Games and Virtual Environment (GVE) for propaganda, recruitment, training, and communication by al-Qaeda fighters. Intelligence sources claimed that al-Qaeda was using these games for these purposes. The NSA agents were able to retrieve chat logs, friendship lists, guildmates, geographical locations, and personal data from the virtual world, which allowed them to plant spyware on targeted computers. The GCHQ and NSA partnered to integrate mapping modules into the World of Warcraft and Xbox Live servers, and the integration was completed by February 2008 (Sáfrán, 2022, p. 187).

Microsoft stated that it only complied with legally valid requests that applied to its users (Makuch, 2013a). The then corporate affairs executive emphasised Microsoft's commitment to protecting its customers' privacy and assured that the company would act if evidence of government surveillance beyond the legal scope was found. In a blog post, he acknowledged customers' concerns regarding government surveillance and stated that "We share their concerns. That's why we are taking steps to ensure governments use legal process rather than technological brute force to access customer data." (Makuch, 2013b).

Following these controversies, Microsoft has taken several steps to make the Xbox network a safer place for gamers. In accordance with a Code of

Conduct applicable to all Microsoft's services, including Xbox Network, it is against the rules to publish terrorist or violent extremist content, convey hate speech, or advocate violence against others (Microsoft, 2022). Xbox has strict community standards that prohibit inappropriate conduct or content, and violators may face temporary or permanent suspensions, forfeiture of licenses, subscriptions, and account balances. The company encourages reporting of inappropriate content and behaviour to take appropriate enforcement action (Microsoft, 2023). Microsoft also joined the European Commission's Code of Conduct initiative to combat online hate speech, resulting in the removal of over 20 million pieces of content from Xbox Live and Mixer in 2019 (EU Counter-Terrorism Coordinator, 2020, p. 15).

YouTube

Since its launch in 2005, YouTube has become the leading platform for sharing videos online, with millions of users able to upload and view videos in any category. Notably, YouTube has emerged as a significant medium for gamers. According to Getomer et al. (2013), the consumption of game-related content on the platform has grown exponentially since 2012. In 2020, YouTube Gaming shattered its previous records, with over 100 billion watch hours and more than 40 million active gaming channels. Major e-sports competitions, including The Call of Duty League, Valorant First Strike, Arena of Valor International Championship, ESL's Counter-Strike Pro League, Overwatch League, League of Legends Worlds, and Free Fire League Championship, have made YouTube their primary venue (Wyatt, 2020).

While live streaming services like Twitch are the most popular for watching others play video games, gamers often post videos to their YouTube channels to recap games and offer predictions for upcoming matches. Minecraft has emerged as a significant influence on YouTube, with the most well-liked channels often featuring Minecraft mods and immersing the viewer in the game's world (Geyser, 2022). There are several Minecraft-related YouTube channels with new videos from those channels consistently getting millions of views. These channels typically focus on gameplay videos, often in the form of "let's play," where the author records themselves while simultaneously narrating the events of a game (Haaranen & Duran, 2017). In 2020, Minecraft gaming videos were watched over 201 billion times, and several content creators saw a massive increase in subscribers and interaction. For instance, Dream's YouTube channel subscriptions surged from 1 million in January 2020 to over 13 million by October of the same year (Wyatt, 2020). This trend has continued over the last two years, and as of December 2022, Dream's channel had over 31 million subscribers.[35]

YouTube has become a platform for highly controversial video games that have been banned from other platforms. These games can be found on the platform as part of "let's play" videos, featuring players who clearly identify with the extreme ideologies in the game and others who denounce the ideologies but still play the games, rating them on their graphics, playability, and storylines (Lakhani, 2021).

[35] https://www.youtube.com/channel/UCTkXRDQloluXxVQrRQvWS6w

References

Anti-Defamation League. (2020). *This is Not a Game: How Steam Harbors Extremists.* https://www.adl.org/resources/report/not-game-how-steam-harbors-extremists

AFP Pakistan. (2021, April 28). This clip actually shows computer-generated imagery from a video game. *AFP Fact Check.* Retrieved from: https://factcheck.afp.com/clip-actually-shows-computer-generated-imagery-video-game-0

AFF Sri Lanka. (2021, May 26). This footage does not show Israel's air defense system — it was mainly created from a video game. *AFP Fact Check.* Retrieved from: https://factcheck.afp.com/footage-does-not-show-israels-air-defense-system-it-was-mainly-created-video-game

Allen, R. (2011). The Unreal Enemy of America's Army. *Games and Culture,* 6(1), 38-60.

Al-Rawi, A. (2018). Video games, terrorism, and Da'esh's Jihad 3.0. *Terrorism and Political Violence,* 30(4), 740–760. https://doi.org/10.1080/09546553.2016.1207633

American Psychiatric Association. (2013). *Diagnostic and statistical manual of mental disorders* (5th ed.). https://doi.org/10.1176/appi.books.9780890425596

American Psychological Association. (2020). *APA Resolution on Violent Video Games.* https://www.apa.org/about/policy/resolution-violent-video-games.pdf

Anderson, A. (2022, February 22). Addressing Health Misinformation. *Discord Blog.* Retrieved from: https://discord.com/blog/addressing-health-misinformation

Anti-Defamation League. (2020). *This is Not a Game: How Steam Harbors Extremists.* https://www.adl.org/resources/report/not-game-how-steam-harbors-extremists

Ball C. & Fordham, J. (2018). Monetization Is the Message: A Historical Examination of Video Game Microtransaction. DiGRA'*18–abstract proceedings of the 2018 DiGRA international conference: The game is the message,* Turin, Italy, 25–28.http://www.digra.org/wp-content/uploads/digital-library/DIGRA_2018_ paper_195.pdf

Barak, M. (2018). "Holy Defense" *Hezbollah's New Computer Game.* [ICT Jihadi Monitoring Group Insights]. International Institute for Counter-Terrorism.

Belding, G. (2021, June 1). In-Game Currency & Money Laundering Schemes: Fortnite, World of Warcraft & More. *Infosec.* Retrieved from: https://resources.infosecinstitute.com/topic/in-game-currency-money-laundering-schemes-fortnite-world-of-warcraft-more/

Ball, J. (2013, December 9). Xbox Live among game services targeted by US and UK spy agencies. *The Guardian.* Retrieved from: https://www.theguardian.com/ world/2013/dec/09/ nsa-spies-online-games-world-warcraft-second-life

Batchelor, J. (2022, March 24). Tencent games revenues rose to $27 billion in 2021. *Games Industry.* Retrieved from: https://www.gamesindustry.biz/tencent-games-revenues-rose-to-usd27-billion-in-2021

Batchelor, J. (2023, January 18). European Parliament votes to take action against loot boxes, gaming addiction, gold farming and more. *Games Industry.* Retrieved from: https://www.gamesindustry.biz/european-parliament-votes-to-take-action-against-loot-boxes-gaming-addiction-gold-farming-and-more

BBC News. (2011, November 11). Valve's online game service Steam hit by hackers. *BBC News.* Retrieved from: https://www.bbc.com/news/technology-15690187

Beck, V. S., Boys, S., Rose, C., & Beck, E. (2012). Violence against women in video games: A prequel or sequel to rape myth acceptance?. *Journal of Interpersonal Violence,* 27(15), 3016–3031. https://doi.org/10.1177/0886260512441078

Bedingfield, W. (2021, August 12). How the far right took over Steam and Discord. *Wired UK.* Retrieved from: https://www.wired.co.uk/article/steam-discord-far-right

Belman, J., & Flanagan, M. (2010). Designing games to foster empathy. International *Journal of Cognitive Technology,* 15(1), 5–15.

Bernevega, A., & Gekker, A. (2022). The Industry of Landlords: Exploring the Assertization of the Triple-A Game. *Games and Culture,* 17(1), 47–69. https://journals.sagepub.com/doi/pdf/10.1177/15554120211014151

Bloom, M., Hicham, T. and Horgan, J. (2017). Navigating Da'esh's Preferred Platform: Telegram. *Terrorism and Political Violence.* DOI:10.1080/09546553.2017.1339695

Boyd, C. (2014, February 18). No, Valve is NOT Collecting your Browsing History. *Malwarebytes Labs.* Retrieved from. https://www.malwarebytes.com/blog/news/2014/02/no-valve-is-not-collecting-your-browsing-history

Brathwaite, B., & Schreiber, I. (2008). *Challenges for Game Designers.* Charles River Media, Boston, Ma.

Burgess, M. C., Stermer, S. P., & Burgess, S. R. (2007). Sex, lies, and video games: The portrayal of male and female characters on video game covers. *Sex Roles,* 57(5–6), 419–433. https://doi.org/10.1007/s11199-007-9250-0

Campbell, C. (2018, March 10). A brief history of blaming video games for mass murder. *Polygon.* Retrieved from: https://www.polygon.com/2018/3/10/17101232/a-brief-history-of-video-game-violence-blame

Campbell, A. (2018, March 8). Steam, Your Kids' Favorite Video Game App, Has A Big Nazi Problem. *The Huffington Post.* Retrieved from: https://www.huffpost.com/entry/steam-video-games-nazis_n_5aa006cae4b0e9381c146438

Castronova, E. (2005). *The Business and Culture of Online Games.* The University of Chicago press.

Carless, W., & Sankin, A. (2018, March 2). The Hate Report: Gaming app has 173 groups that glorify school shooters. *Reveal.* Retrieved from: http://revealnews.org/blog/hate-report-gaming-app-has-173-groups-that-glorify-school-shooters/

Chalk, A. (2022, February 9). America's Army is finally closing for good. *PC Gamer.* Retrieved from: https://www.pcgamer.com/americas-army-is-finally-closing-for-good/

Chokshi, N. (2017, February 14). Disney Drops PewDiePie and YouTube Distances Itself After Reports of Anti-Semitic Videos. *The New York Times.* Retrieved from: https://www.nytimes.com/2017/02/14/business/pewdiepie-youtube-disney.html

Close, J., & Lloyd, J. (2021). *Lifting the lid on loot-boxes: Chance-based purchases in video games and the convergence of gaming and gambling.* London, UK: University of Plymouth and University of Wolverhampton on behalf of GambleAware. Retrieved from: https://www.begambleaware.org/sites/default/files/2021-07/Gaming_and_Gambling_Report_Final_0.pdf

Cohen, L. (2020, January 1). White nationalists are moving from YouTube to DLive. *The Daily Dot.* Retrieved from: https://www.dailydot.com/upstream/dlive-streaming-white-nationalism/

Conell, J. (2023, January 31). ToxMod's Powerful Voice Moderation is Now Available on Nintendo Switch. *Modulate.* Retrieved from: https://www.modulate.ai/blog/toxmod-voice-moderation-nintendo-switch

Coontz, L. (2022, March 14.) How Video Game Footage Is Being Used in The Propaganda Wars. *Coffee or Die Magazine*.
Retrieved from: https://coffeeordie.com/video-game-footage-propaganda/

Conditt, J. (2013, January 23). Black Ops 2, Warfighter banned in Pakistan for depicting country in "very poor light". *Engadget*.
Retrieved from: https://www.engadget.com/2013-01-23-black-ops-2-warfighter-banned-in-pakistan-for-depicting-country.html

Conditt, J. (2020, May 15). A closer look at Valorant's always-on anti-cheat system. *Engadget*. Retrieved from: https://www.engadget.com/valorant-vanguard-riot-games-security-interview-video-170025435.html

Cotter, E. (2022, November 3). Money Laundering Through Video Games. Napier *Technologies Limited*. Retrieved from: https://www.napier.ai/post/money-laundering-gaming-industry

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

Crump, E. (2015). Turn That Game Back On: Video Games, Violence and the Myth of Injury to the Public Good. *Auckland University Law Review,* Vol. 20, 171–194.

Curry, D. (2023, February 22). Mobile Games Revenue Data (2023). *Business of Apps*. Retrieved from: https://www.businessofapps.com/data/mobile-games-revenue/

Cuthbertson, A. (2019, January 13). How Children Playing Fortnite are Helping to Fuel Organised Crime. *The Independent*. Retrieved from: https://www.independent.co.uk/news/fortnite-v-bucks-discount-price-money-dark-web-money-laundering-crime-a8717941.html

Dauber, C. E., Robinson, M. D., Baslious, J. J., & Blair, A. G. (2019). Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos. *Perspectives on Terrorism,* 13(3), 17–31.
https://www.jstor.org/stable/26681906

Davey, J. (2021). Gamers who hate: *An introduction to ISD's gaming and extremism series*. Institute for Strategic Dialogue. https://www.isdglobal.org/wp-content/uploads/2021/09/20210910-gaming-reportintro.pdf

Dataspelsbranschen. (2022). *Spelutvecklarindex 2022*.
https://static1.squarespace.com/static/5a61edb7a803bb7a65252b2d/t/636e920a2cb5d660a852bd73/1668190740696/Spelutvecklarindex2022-SV-WEBB.pdf

Darvasi, P. (2016). "Empathy, perspective, and complicity: How digital games can support peace education and conflict resolution." In M. Faetanini & R. Tankha (Eds.), *Social inclusion of internal migrants in India: Internal migration in India initiative.* United Nations Educational Scientific and Cultural Organization.

Darvesh, N., Radhakrishnan, A., Lanchance, C. C., Nincic, V., Ghassemi, M., Straus, S. E., & Tricco, A. C. (2020). Exploring the prevalence of gaming disorder and Internet gaming disorder: a rapid scoping review. *Systematic Reviews,* (9) 68, https://doi.org/10.1186/s13643-020-01329-2

Dean. (2021, April 13). Steam Usage and Catalog Stats for 2022. *Backlinko.*
Retrieved from: https://backlinko.com/steam-users

DeLisi, M., Vaughn, M. G., Gentile, D. A., Graig, A. A., & Shook, J. J. (2013). Violent Video Games, Delinquency, and Youth Violence: New Evidence. *Academy of Criminal Justice Science,* 11(2),
https://doi.org/10.1177/154120401246087 4

Delwiche, A. (2007). "From The Green Berets to America's Army: Video Games as a Vehicle for Political Propaganda". In Williams, J. P., & Smith, J. H. *The player's realm: Studies on the culture of video games and gaming.*
Jefferson, N.C: McFarland & Co.

Denton, J. (2022, August 15). China Is Infiltrating Kids' Video Games With Propaganda and Spyware. *Heritage*.
Retrieved from: https://www.heritage.org/technology/commentary/china-infiltrating-kids-video-games-propaganda-and-spyware

Deterding, S., Dixon, D., Khaled, R. and Nacke, L. (2011). From Game Design Elements to Gamefulness: Defining Gamification. *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments.* http://dx.doi.org/10.1145/2181037.218104

Department of Justice. (2021, August 26). *Four Charged in Alleged $150 Million Payment Processing Scheme*. [Press release]. https://www.justice.gov/opa/pr/four-charged-alleged-150-million-payment-processing-scheme

Dhar, A. (2020, November 1). Fortnite: The Biden-Harris campaign and the Build Back Better map. *Sportskeeda.* Retrieved from:
https://www.sportskeeda.com/fortnite/fortnite-the-biden-harris-campaign-build-back-better-map

Discord. (2022). *Discord Transparency Report: April – June 2022*.
https://discord.com/blog/discord-transparency-report-q2-2022

DLive Community. (2021, March 8). Service Guidelines · DLive Community. *DLiveCommunity.* https://community.dlive.tv/about/community-guidelines/

EarlyGame. (2020a, September 3). *PUBG Mobile Banned in India, Call of Duty to Follow?* [Press release]. https://earlygame.com/pubg-mobile-banned-in-india-call-of-duty-to-follow

EarlyGame. (2020b, November 16). *PUBG Mobile India's Censorship Is Bollocks.* [Press release]. https://earlygame.com/gaming/pubg-mobile-india-censorship

Egliston, B. (2022, February 1). The Unnerving Rise of Video Games that Spy on You. *Wired.* Retrieved from: https://www.wired.com/story/video-games-data-privacy-artificial-intelligence/

Eisele, I. (2022, April 4). Fact check: The 'Ghost of Kyiv' fighter pilot. DW. Retrieved from: https://www.dw.com/en/fact-check-ukraines-ghost-of-kyiv-fighter-pilot/a-60951825

Elder, M. (2013, June 11). Russia passes law banning gay "propaganda". *The Guardian.* Retrieved from: https://www.theguardian.com/world/2013/jun/11/russia-law-banning-gay-propaganda

Engelhardt, C. R., Bartholow, B. D., Kerr, G. T., & Bushman, B. J. (2011). This is your brain on violent video games: Neural desensitization to violence predicts increased aggression following violent video game exposure. *Journal of Experimental Social Psychology.* https://doi.org/10.1016/j.jesp.2011.03.027

EU Counter-Terrorism Coordinator. (2020). 9066/20. *Online gaming in the context of the fight against terrorism.* Council of the European Union. Retrieved from: https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf

European External Action Service. (2023). *1st EEAS Report on Foreign Information Manipulation and Interference Threats.* https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf

European Parliament. (2022). *Consumer protection in online video games: a European Single Market approach* (2022/2014(INI)). https://www.europarl.europa.eu/doceo/document/IMCO-PR-719799_EN.pdf

Europol. (2021). *EU Terrorism Situation & Trend Report.* Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat

Rogers, E. M., & Larsen, J. L. (1984). *Silicon Valley fever: growth of high-technology culture.* Basic Books

Ferguson, C. J. (2015). Does Movie or Video Game Violence Predict Societal Violence? It Depends on What You Look at and When. *Journal of Communication,* 65(1), 193–212. https://doi.org/10.1111/jcom.12142

Flanagan, M. (2009). *Critical play: Radical game design.* The MIT Press.

Folkhälsomyndigheten. (2022). Resultat från regeringsuppdrag att genomföra en befolkningsstudie om spel om pengar. https://www.folkhalsomyndigheten.se/contentassets/58e8320a52944ef8bd2b013e068e2c5e/resultat-fran-regeringsuppdrag-att-genomfora-en-befolkningsstudie-om-spel.pdf

Foust, J. (2021, March 25). Video games are the new contested space for public policy. *Brookings.* Retrieved from: https://www.brookings.edu/techstream/video-games-are-the-new-contested-space-for-public-policy/

Foust, J. (2022, Oktober 20). Video game censorship is authoritarians' latest tool to muzzle speech. *Brookings.* Retrieved from: https://www.brookings.edu/techstream/video-games-censorship-free-speech-authoritarianism-china-russia/

Foust, J., & Jerome, J. (2021, June 25). A guide to reining in data-driven video game design. *Brookings.* Retrieved from: https://www.brookings.edu/techstream/a-guide-to-reining-in-data-driven-video-game-design-privacy/

Franceschi-Bicchierai. (2023a, February 21). Hackers steal Activision games and employee data. *TechCrunch.* Retrieved from: https://techcrunch.com/2023/02/21/hackers-allegedly-steal-activision-games-and-employee-data/

Francheschi-Bicchierai. (2023b, January 24). Riot Games hack could help cheaters. *TechCrunch.* Retrieved from: https://techcrunch.com/2023/01/24/riot-games-hack-cheaters/?&web_view=true#!

Friedberg, J. (2015). Gender Games: *A Content Analysis Of Gender Portrayals In Mo Narrative Video Games.* [Thesis, Georgia State University]. https://doi.org/10.57709/7000435

Funk, J. B., Buchman, D. D., Jenks, J., & Bechtoldt, H. (2003). Playing violent video games, desensitization, and moral evaluation in children. *Journal of Applied Developmental Psychology,* 24(4), 413–436. https://doi.org/10.1016/S0193-3973(03)00073-X

Gais, H., & Edison Hayden, M. (2020, November 17). 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

Gallagher, A., O'Connor, C., Vaux, P., Thomas, E., & Davey, J. (2021). Gaming and Extremism: *The Extreme Right on Discord.* Institute for Strategic Dialogue. https://www.isdglobal.org/isd-publications/gaming-and-extremism-the-extreme-right-on-discord/

Gao, Y. X., Wang, J. Y., & Dong, G. H. (2022). The prevalence and possible risk factors of internet gaming disorder among adolescents and young adults: Systematic reviews and meta-analyses. *Journal of psychiatric research,* 154, 35–43. https://doi.org/10.1016/j.jpsychires.2022.06.049

Gardner, M. (2019, September 12). British MPs Demand Loot Box "Gambling" Ban For Young Gamers. *Forbes.* Retrieved from: https://www.forbes.com/sites/mattgardner1/2019/09/12/british-mps-demand-loot-box-gambling-ban-for-young-gamers/?sh=181f7a58302b

Gee, J. (2005). Learning by Design: Good Video Games as Learning Machines. *E-learning,* 2. https://doi.org/10.2304/elea.2005.2.1.5

Geyser, W. (2022). The Top 20 *Gaming Influencers on Youtube [by Subscriber Count].* Influencer Marketing Hub. https://influencermarketinghub.com/gaming-influencers/

Gershenfeld, A., & Angst, M. (2021, September 13). Exploring and extending world cultures through video games. *Creativity, Culture & Capital.* Retrievedfrom: https://www.creativityculturecapital.org/blog/2021/09/13/exploring-and-extending-world-cultures-through-video-games/

Getomer, J., Okimoto, M., & Johnsmeyer, B. (2013). *Gamers on Youtube: Evolving Video Consumption.* https://www.thinkwithgoogle.com/_qs/documents/261/youtube-marketing-to-gamers_articles.pdf

Grand View Research. (2021). *Esports Market Size, Share & Trends Analysis Report By Revenue Source (Sponsorship, Advertising, Merchandise & Tickets, Media Rights),* By Region, And Segment Forecasts, 2022 – 2030. Retrieved from: https://www.grandviewresearch.com/industry-analysis/esports-market

Granic, I., Lobel, A., & Engels, R. (2014). The Benefits of Playing Video Games. *American Psychologist,* 69(1): 66-78. DOI: 10.1037/a0034857

Greig, M. (2021, July 9). Tencent Uses Facial Recognition to Ban Kids Gaming Past Bedtime. *Bloomberg.* Retrieved from: https://www.bloomberg.com/news/articles/2021-07-08/tencent-uses-facial-recognition-to-ban-kids-gaming-past-bedtime?leadSource=uverify%20wall

Greitemeyer, T. (2014). Intense acts of violence during video game play make daily life aggression appear innocuous: A new mechanism why violent video games increase aggression. *Journal of Experimental Social Psychology,* 50(1), 52–56.

Gualt, M. (2016, August 13). 'Supreme Ruler Ultimate: Trump Rising' let's you rule America as The Donald. *Vice.* Retrieved from: https://www.vice.com/en/article/ yp3xzm/supreme-ruler-trump

Guhl, J., Ebner, J., & Rau, J. (2020). *The Online Ecosystem of the German Far-Right.* Institute for Strategic Dialogue. https://www.isdglobal.org/wp-content/uploads/2020/02/ISD-The-Online-Ecosystem-of-the-German-Far-Right-English-Draft-11.pdf

Haaranen, L., & Duran, R. (2017). Link Between Gaming Communities in YouTube and Computer Science. *Department of Computer Science, Aalto University, Helsinki, Finland, Proceedings of the 9th International Conference on Computer Supported Education,* 2, 17–24. https://doi.org/10.5220/0006267000170024

Harris, K. A. (2016). The New Black Face: The Transition of Black One-Dimensional Characters from Film to Video Games. *Southern Illinois University Carbondale.*

Hasler, B. S., Hirschberger, G., Shani-Sherman, T., & Friedman, D. A. (2014). Virtual Peacemakers: Mimicry increases empathy in simulated contact with virtual outgroup members. *Cyberpsychology, Behavior, and Social Networking,* 17(12), 766–771. https://doi.org/10.1089/cyber.2014.0213

Higgins, E. (2017, November 14). The Russian Ministry of Defence Publishes Screenshots of Computer Games as Evidence of US Collusion with Da'esh. *Bellingcat.* Retrieved from: https://www.bellingcat.com/news/mena/2017/11/14/russian-ministry-defence-publishes-screenshots-computer-games-evidence-us-collusion-Da'esh/

Hollister, S. (2020, September 15). Xbox Game Pass briefly explained: console, PC, xCloud streaming and more. *The Verge.* Retrieved from: https://www.theverge.com/2020/9/15/21437529/xbox-game-pass-versions-tier-ultimate-pc-console-explainer

Holmes, O. (2021, July 15). No cults, no politics, no ghouls: How China censors the video game world. *The Guardian.* Retrieved from: https://www.theguardian.com/news/2021/jul/15/china-video-game-censorship-tencent-netease-blizzard

Ikeda, S. (2019, December 30). Password Breach of Game Developer Zynga Compromises 170 Million Accounts. *CPO Magazine.* Retrieved from: https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/

Institute for Strategic Dialogue. (2020). Bankrolling Bigotry: *An Overview of the Online Funding Strategies of American Hate Groups.* https://www.isdglobal.org/wp-content/uploads/2020/10/bankrolling-bigotry-3.pdf

Jiow, H. J., Lye, Q., & Woo, K. (2019). Not Yet Game Over: A Reappraisal of Video Game Addiction. *The Journal of the Canadian Game Studies Association,* 12(19): 1-17. http://dx.doi.org/10.7202/1058317ar

Jin, Y., Qin, L., Zhang, H., & Zhang, R. (2021). Social Factors Associated with Video Game Addiction Among Teenagers: School, Family and Peers. Advances in Social Science, *Education and Humanities Research.* https://doi.org/10.2991/assehr.k.211220.131

Kaati, L., Omer, E., Prucha, N. and Shrestha, A. (2015). *Detecting Multipliers of Jihadism on Twitter.* The Swedish Defence Research Agency. https://www.foi.se/download/18.7fd35d7f166c56ebeob1000c/1542623725677/Detecting-multipliers-of-jihadism_FOI-S--5656--SE.pdf

Kaplan, S. (2014, September 12). With #GamerGate, the Video-Game Industry's Growing Pains Go Viral. *The Washington Post.* Retrieved from: https://www.washingtonpost.com/news/morning-mix/wp/2014/09/12/with-gamergate-the-video-game-industrys-growing-pains-go-viral/

Kaspersky. (2022). *Good game, well played: an overview of faming-related cyberthreats in 2022.* Kaspersky. https://securelist.com/gaming-related-cyberthreats-2021-2022/107346/

Kelly, S. (2021). Money Laundering through Virtual Worlds of Video Games: Recommendations For a New Approach to AML Regulation. *Syracuse Law Review,* 71

Kowert, R., & Quandt, T. (Eds.). (2016). *The video game debate: Unravelling thephysical, social, and psychological effects of digital games.* Oxon: Routledge.

Kowert, R., Martel, A., & Swann, B. (2022) Not just a game: Identity fusion and extremism in gaming culture. *Frontiers in Psychology.* Vol. 7. https://doi.org/10.3389/fcomm.2022.1007128

Kretzschmar, M., & Stanfill, M. (2019). Mods as Lightning Rods: A Typology of Video Game Mods, Intellectual Property, and Social Benefit/Harm. *Social & Legal Studies,* 28(4). https://doi.org/10.1177/0964663918787221

Kröger, J. L., Raschke, P., Campbell, J. P., & Ullrich, S. (2021). Surveilling the Gamers: Privacy Impacts of the Video Game Industry. *Video Game Industry, Entertainment Computing,* Vol 44. https://doi.org/10.1016/j.entcom.2022.100537

Lakhani, S. (2021). *Video gaming and (violent) extremism: An exploration of the current landscape, trends, and threats.* European Commission. https://home-affairs.ec.europa.eu/system/files/2022-02/EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20RAN%20Policy%20Support%20paper_en.pdf

Lakomy, M. (2019). Let's Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment. *Studies in Conflict & Terrorism,* 42(4), 383–406. https://doi.org/10.1080/1057610X.2017.1385903

Lamphere-Englund, G., & Bunmathong, L. (2022). *State of Play Report: Reviewing the Literature on Gaming & Extremism.* Extremism and Gaming Research Network.

Lambert, H. (2023, January 18). Statement on European Parliament vote on report "Consumer protection in online video games – a European single market approach". *Europe's Video Games Industry.* Retrieved from: https://www.isfe.eu/news/isfe-egdf-statement-on-european-parliament-vote-on-report-consumer-protection-in-online-video-games-a-european-single-market-approach/

Lee, B. (2021, November 17). Only Playing: Extreme-Right Gamification. *VoxPol.* Retrieved from: https://www.voxpol.eu/only-playing-extreme-right-gamification/

Lewis, R. (2014, July 15). The hacker who went to war with Riot Games. *Dot Esports.* Retrieved from: https://dotesports.com/league-of-legends/news/jason-shane-duffy-league-of-legends-hacks-464

Liao, S. (2019, March 4). Over 300 million Chinese private messages were left exposed online. *TheVerge.* Retrieved from: https://www.theverge.com/2019/3/4/18250474/chinese-messages-millions-wechat-qq-yy-data-breach-police

Lin, J.H. (2013). Identification Matters: A Moderated Mediation Model of Media Interactivity, Character Identification, and Video Game Violence on Aggression. *Journal of Communication,* 63(4), 682–702. https://doi.org/10.1111/jcom.12044

Lishchuk, R. (2021, June 23). 6 Major Data Breaches We Found and Reported in 2018. *MacKeeper.* Retrieved from: https://mackeeper.com/blog/data-breach-reports-2018/

Lockheed Martin. (2020). *How Gaming Technology Helps Missiles Go Over Mach 5.* Lockheed Martin. Retrieved from: https://www.lockheedmartin.com/en-us/news/features/2020/How-Gaming-Technology-Helps-Missiles-Go-Over-Mach-5.html

Lutkevich, B. (2023). What is virtual reality gaming (VR gaming)? *TechTarget.* Retrieved from: https://www.techtarget.com/whatis/definition/virtual-reality-gaming-VR-gaming

Luxembourg House of Cybersecurity. (2022). Esports and its Cyber Threats – Why Is Esports an Attractive Target? *Luxembourg House of Cybersecurity.* Retrieved from: https://securitymadein.lu/cyber/topic-of-the-month/esports-and-its-cyber-threats/

MacDonald, K. (2016, December 7). Russian MPs are not the first to try to write LGBT people out of video games. *The Guardian.* Retrieved from: https://www.theguardian.com/commentisfree/2016/dec/07/russian-mps-lgbt-out-video-games

Macklin, G. (2019). The Christchurch Attacks: Livestream Terror in the Viral Video Age. *CTC Sentinel,* 12(6)

Makuch, E. (2013a, December 5). Microsoft blasts "government snooping," pledges to enhance encryption. *GameSpot.* Retrieved from: https://www.gamespot.com/articles/microsoft-blasts-government-snooping-pledges-to-enhance-encryption/1100-6416565/

Makuch, E. (2013b, December 9). Government infiltrates Xbox Live and World of Warcraft in search of terrorists. *GameSpot.* Retrieved from: https://www.gamespot.com/articles/government-infiltrates-xbox-live-and-world-of-warcraft-in-search-of-terrorists/1100-6416610/

Maiberg, E. (2017, October 19). Steam Is Full of Hate Groups. *Vice.* Retrieved from: https://www.vice.com/en/article/d3dzvw/steam-is-full-nazi-racist-groups

Mahmoud, F. (2022). *The gamification of jihad.* Danish Institute for International Studies. https://www.diis.dk/en/research/new-report-explores-the-field-between-gaming-jihadism

McCarthy, K. K. (2015). Revealing a Spectrum of Racialised Sexuality: Representations of Video Game Characters Over Time, 1981-2012. *University of New Mexico.*

Menegus, B. (2022, January 30). What's the Deal With Anti-Cheat Software in Online Games? *Wired.* Retrieved from: https://www.wired.com/story/kernel-anti-cheat-online-gaming-vulnerabilities/

Messner, S. (2020, August 9). Every game company that Tencent has invested in. *PC Gamer.* Retrieved from: https://www.pcgamer.com/every-game-company-that-tencent-has-invested-in/

Microsoft. (2002, November 15). Xbox Live Arrives in Stores, Sparking the Next Revolution in Video Games. [Press release]. Retrieved from: https://news.microsoft.com/2002/11/15/xbox-live-arrives-in-stores-sparking-the-next-revolution-in-video-games/

Microsoft (2023). XBOX Bounty Program. Microsoft. Retrieved from: https://www.microsoft.com/en-us/msrc/bounty-xbox

Milburn, C. (2018). *Gamers, Hackers, and Technogenic Life.* Duke University Press, Durham and London. https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/22280/9781478090366_OA.pdf?sequence=1&isAllowed=y

Ministry of Defence & Defence and Security Accelerator. (2020, March 6). Gaming technology trialled in training UK Armed Forces. [Press release]. Retrieved from: https://www.gov.uk/government/news/gaming-technology-trialled-in-training-uk-armed-forces

Mirkasymov, R., & Martinez, R. (2022, August 25). Roasting oktapus: The phishing campaign going after Okta identity credentials. *Group-IB.* Retrieved from: https://www.group-ib.com/blog/oktapus/

Modulate. (n.d.). ToxMod. *Modulate.* Retrieved from: https://www.modulate.ai/tox-mod

Moiseienko, A., & Isenman, K. (2019). Gaming the System: Money Laundering Through Online Games. *RUSI Newsbrief,* 39(9). https://static.rusi.org/20191011_newsbrief_vol39_no9_moiseienko_and_isenman_web.pdf

Mou, Y., & Wei P. (2009). "Gender and racial stereotypes in popular video games." In Ferding, R. E. (Ed.), *Handbook of research on effective electronic gaming in education.* University of Florida, USA. http://dx.doi.org/10.4018/9781599048086.ch053

Nasr, A. (2016, March 10). Anti-Terror Group Pressures Sony About PlayStation Network. *Morning Consult.* Retrieved from: https://morningconsult.com/2016/03/10/exclusive-nonprofit-seeks-answers-from-sony-on-terrorists-and-playstation/

Souri, H. T. (2007). The political battlefield of pro-Arab video games on Palestinian screens. *Comparative Studies of South Asia, Africa and the Middle East,* 27(3), 536–551. https://doi.org/10.1215/1089201x-2007-031

Newman, J., Jerome, J. W., & Hazard, C. J. (2014). Press Start to Track?: Privacy and the New Questions Posed by Modern Videogame Technology. *American Intellectual Property Law Association* (AIPLA) Quarterly Journal

Nieborg, D. B. (2004). "America's Army: More than a game". In Eberle, T., & Kriz, C. (Eds.), *Transforming Knowledge into Action through Gaming and Simulation,* München: SAGSAGA, CD-ROM

Nintendo. (n.d.) Nintendo Switch Online. https://www.nintendo.com/switch/online/nintendo-switch-online/

Nothhaft, H., Pamment, J. Agardh-Twetman, H., Fjällhed, A. (2018) Information Influence in Western Democracies: A model of systemic vulnerabilities. In Bjola, C. & Pamment, J. (2018) *Countering Online Propaganda and Violent Extremism: The Dark Side of Digital Diplomacy.* Oxon: Routledge

Pamment, J., Nothhaft, H., Agardh-Twetman., & Fjällhed, A. (2018). *Countering Information Influence Activities: The State of the Art.* MSB. https://www.msb.se/RibData/Filer/pdf/28697.pdf

Pagan, E. (2019, December 1). Designing Interactivity into Game Play. *University of Silicon Valley.* Retrieved from: https://usv.edu/blog/designing-interactivity-into-game-play/

Page, C. (2023, February 10). Reddit says hackers accessed employee data following phishing attack. *TechCrunch*. Retrieved from: https://techcrunch.com/2023/02/10/reddit-says-hackers-accessed-internal-data-following-employee-phishing-attack/

Pearson, J., & Horwitz, J. (2018, August 2). How a business serving bettors, porn donated to Dems, Trump. *The Associated Press*. Retrieved from: https://www.google.com/search?q=Four+Charged+in+Alleged+%24150+Million+Payment+Pro-cessing+Scheme+prepaid+cards&rlz=1C5CHFA_enSE902SE902&sxsrf=APwXEd-crr0z9mTnHaSiATX71ubqlXsSpJw:1681818716105&ei=XIQ-ZN2FBseRxc8PlYqB-gAk&start=10&sa=N&ved=2ahUKEwjd05n5rrP-AhXHSPEDHRVFAJAQ8tMDeg-QIBhAE&biw=714&bih=788&dpr=2

Perez Latorre, O. (2015). The Social Discourse of Video Games Analysis Model and Case Study: GTA IV. *Games and Culture,* 10(5), 415–437. https://doi.org/10.1177/1555412014565639

Perry, T. (2007, august 16). Hezbollah brings Israel war to computer screen. *Reuters*. Retrieved from: https://www.reuters.com/article/idUSL16624293

Plaum, A. (2020, September 3). Fighting the infodemic, one game at a time. *Innovation*. Retrieved from: https://innovation.dw.com/articles/fighting-the-infodemic-one-game-at-a-time

PlayStation. (n.d.). *Tjänstevillkor för PlayStation Network*. Retrieved from: https://www.playstation.com/sv-se/legal/psn-terms-of-service/

Prell, S. (2017, June 14). Xbox One Avatars will support wheelchairs, prosthetic limbs, pregnancy, unicorns, and a lot more. *GamersRadar.* Retrieved from: https://www.gamesradar.com/xbox-one-avatars-will-support-wheelchairs-prosthetic-limbs-pregnancy-unicorns-and-a-lot-more/

Przybylski, A. K., Ryan, R. M., & Rigby, C. S. (2009). The Motivating Role of Violence in Video Games. *Personality and Social Psychology Bulletin,* 35(2), 243–259. https://doi.org/10.1177/0146167208327216

Przybylski, A. K., Weinstein, N., & Murayama, K. (2017). Internet Gaming Disorder: Investigating the Clinical Relevance of a New Phenomenon. *The American journal of psychiatry,* 174(3), 230–236. https://doi.org/10.1176/appi.ajp.2016.16020224

Quinn, B., & Arthur, C. (2011, April 26). PlayStation Network hackers access data of 77 million users. *The Guardian*. Retrieved from: https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data

Revoredo, T. (2022, January 22). Blockchain and The Evolution of Business Models in the Game Industry. *Cointelegraph*. Retrieved from: https://cointelegraph.com/news/blockchain-and-the-evolution-of-business-models-in-the-game-industry

Reymann-Schneider. (2020, October 19). How video games are used for political purposes. *DW*. Retrieved from: https://www.dw.com/en/how-politicians-use-video-games-for-their-own-gains/a-55286753

Reynolds, A. (2022, November 16). *Blizzard Entertainment and NetEase Suspending Game Services in China.* [Press release]. https://investor.activision.com/news-releases/news-release-details/blizzard-entertainment-and-netease-suspending-game-services

Ritterfeld, U., Cody, M. J., & Vorderer, P. (Eds.). (2009). *Serious Games: Mechanisms and Effects*. Routledge.

Roach, J. (2020, October 13). What is DRM in video games and how does it work? *Digitaltrends*. Retrieved from: https://www.digitaltrends.com/gaming/what-is-drm-in-video-games/

Roach, J., & Yaden, J. (2022, April 27). Everything you need to know about Nintendo Switch Online. *Digitaltrends*. Retrieved from: https://www.digitaltrends.com/gaming/everything-you-need-to-know-nintendo-switch-online/

Rodríguez Espínola, A. (2021). *Video Games as Tools for Non-State Cultural Diplomacy: A Case Study of the Video Game Never Alone.* [Doctoral dissertation, University of Colorado Boulder]. https://scholar.colorado.edu/concern/graduate_thesis_or_dissertations/4x51hk28f

Rosenberg, L. (2023, January 1). 2023 could be the year of mixed reality. *VentureBeat*. Retrieved from: https://venturebeat.com/virtual/2023-could-be-the-year-of-mixed-reality/

Ruby, D. (2023, March 10). 44+ eSports Statistics for 2023 (Trends, Facts & Insights). *Demand Sage*. Retrieved from: https://www.demandsage.com/esports-statistics/

Russell, N. C., Reidenberg,, . R., & Sumyung, M. (2019). Privacy in Gaming. *Fordham Intellectual Property, Media & Entertainment Law Journal,* 29(1), 61-180. https://ir.lawnet.fordham.edu/iplj/vol29/iss1/4

Russworm, T. (2017). "Dystopian Blackness and the Limits of Racial Empathy in the Walking Dead and in The Last of Us". In Malowski, J., & Russworn, T. (Eds.), *Game Representation: Race, Gender, and The Sexuality,* Video Games Bloomington, IN: Indiana University Press, Inc. https://doi.org/10.2307/j.ctt2005rgq

Sáfrán, J. (2022). Digital Terrorism: Communication through Online Video Games. *Military Science Review,* 15(3), 183–195. DOI:10.32563/HSZ.2022.3.12

Salter, M. B. (2011). The Geographical Imaginations of Video Games: Diplomacy, Civilization, America's Army and Grand Theft Auto IV. *Geopolitics,* 16(2), 359-388.

Sautman, M.,Misagh, S., Gadus, I., & Jenae, L. M. (2017, February 26). Story Telling and Interactivity in Video Gaming. *The Artifice*. Retrieved from: https://the-artifice.com/video-gaming-story-telling-interactivity/

Schlegel, L. (2020). Jumanji Extremism? How games and gamification could facilitate radicalization processes. *Journal for Deradicalization,* 23. https://journals.sfu.ca/jd/index.php/jd/article/view/359

Schlegel, L. (2021a). *The gamification of violent extremism & lessons for P/CVE*. Radicalization Awareness Network. https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/publications/gamification-violent-extremism-lessons-pcve-2021_en

Schlegel, L. (2021b). *Extremists' use of gaming (adjacent) platforms.* Radicalization Awareness Network & European Commission. Luxembourg: Publications Office of the European Union. https://home-affairs.ec.europa.eu/system/files/2021-08/ran_extremists_use_gaming_platforms_082021_en.pdf

Schlegel, L. (2022). *Examining the Intersection Between Gaming and Violent Extremism.* United Nations Office of Counter-Terrorism (UNCCT.). https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/221005_research_launch_on_gaming_ve.pdf

Schulzke, M. (2013). Rethinking Military Gaming: America's Army and Its Critics. *Games and Culture,* 8(2), 59-76. https://doi.org/10.1177/1555412013478686

Sherer, J. (2023, January). Internet Gaming. *American Psychiatric Association.* Retrieved from: https://www.psychiatry.org/patients-families/internet-gaming

Sony. (2011, May 17). PlayStation Network Restoration Begins. [Press release]. Retrieved from: https://web.archive.org/web/20160303222252/http://uk.playstation.com/psn/news/articles/detail/item369506/PSN-Qriocity-Service-Update/

Sony. (2014, December 8). December 8, 2014. [Summary of SPE's prior communication]. Retrieved from: https://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf

Steam. (2018a). Who Gets To Be On The Steam Store. Retrieved from: https://store.steampowered.com/news/group/27766192/view/Steam.

Steam (2018b). Steam Discussions—Moderation Update. [Press release]. Retrieved from: https://store.steampowered.com/news/group/4145017/view/

Steam. (2019). Rape Day will not ship on Steam. [Press release]. Retrieved from:https://store.steampowered.com/news/group/27766192/view/

Svenska E-sportförbundet. (n.d.). *Vad är E-sport?* Svenska E-sportförbundet. Retrieved from: https://www.svenskesport.se/esport

Squire, M. (2021). Monetizing Propaganda: How Far-right Extremists Earn Money by Video Streaming. *WebSci '21: 13th International ACM Conference on Web Science in 2021,* June 21–25, 2021. ACM, New York, NY, USA, https://doi.org/10.48550/arXiv.2105.05929

Talbert, J. (2016). A Gatekeeper Final Boss: An Analysis of MOGAI Representation in Video Games.

The German Games Industry Association. (2021, March 10). German Bundestag passes new Youth Protection Act. *The German Games Industry Association.* Retrieved from: https://www.game.de/en/german-bundestag-passes-new-youth-protection-act/

The European Games Developer Federation (EGDF) & Europe's Video Games Industry (ISFE). (2022). *Key Facts From 2021.* Retrieved from: https://www.isfe.eu/wp-content/uploads/2022/08/FINAL-ISFE-EGDFKey-Facts-from-2021-about-Europe-video-games-sector-web.pdf

The National Security Agency. (2011, December 9). NSA Launches New Crypto Mobile Game App. [Press release]. Retrieved from: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1630529/nsa-launches-new-crypto-mobile-game-app/

Swedish Civil Contingencies Agency. (2018). *Countering information influence activities – A handbook for communicators.* https://www.msb.se/ribdata/filer/pdf/28698.pdf

Thomala, L. L. (2022). *Tencent: Online games revenue* 2021.

Thomas, E. (2021). *The Extreme Right on DLive*. Institute for Strategic Dialogue. https://www.isdglobal.org/isd-publications/gaming-and-extremism-the-extreme-right-on-dlive/

Thulin, L. (2018, March 26). The Roots of the Cambridge Analytica Scandal. *Slate.* Retrieved from: https://slate.com/technology/2018/03/farmville-helped-sow-the-seeds-of-the-cambridge-analytica-scandal.html

Tidy, J. (2022, September 30). Roblox removes 'meat grinder' Ukraine v Russia game. *BBC News.* Retrieved from: https://www.bbc.com/news/technology-63078950

TrendLabs. (2016). *The Cybercriminal Roots of Selling Online Gaming Currency.* https://documents.trendmicro.com/assets/wp/wp-cybercrime-online-gaming-currency.pdf

Twitch. (2021). *Transparency Report 2020.* https://safety.twitch.tv/s/article/Transparency-Reports?language=en_US

Twitch. (2022a). *H1 2022 Transparency Report.* https://safety.twitch.tv/s/article/H1-2022-Transparency-Report?language=en_US

Twitch. (2022b). *H2 2021 Transparency Report.* https://safety.twitch.tv/s/article/H2-2021-Transparency-Report?language=en_US

Twitch. (2022c). Preventing Harmful Misinformation Actors on Twitch. https://safety.twitch.tv/s/article/Preventing-Misinformation-Actors-from-Using-Twitch?language=en_US

Valve. (2019, October 28). Key Change. [Press release]. Retrieved from: https://blog.counter-strike.net/index.php/2019/10/26113/

Vaux, P., Gallagher, A., & Davey, J. (2021). *The Extreme Right on Steam.* Institute for Strategic Dialogue. https://www.isdglobal.org/wp-content/uploads/2021/08/02-revised-gaming-report-steam.pdf

Vega, A. (2023, March 10). The Rise of Mobile Gaming: A Look at the Growing Industry. *LinkedIn.* Retrieved from: https://www.linkedin.com/pulse/rise-mobile-gaming-look-growing-industry-axel-vega/

Warren, T. (2021, January 26). Xbox Game Pass subscribers hit 18 million. *The Verge.* Retrieved from: https://www.theverge.com/2021/1/26/22250795/xbox-game-pass-subscribers-growth-microsoft

Webb, J., & Davies, R. (2022, October 11). Diversity in video games: the best (and worst) examples of representation. *Evening Standard.* Retrieved from: https://www.standard.co.uk/tech/gaming/video-game-diversity-representation-a44461266.html

Webber, J. E. (2016, November 29). Inside a virtual war: can video games recreate life in a conflict-ridden city? *The Guardian.* Retrieved from: https://www.theguardian.com/cities/2016/nov/29/this-war-of-mine-video-game-about-life-cities-war

Weimann, G. (2010). Terror on Facebook, Twitter, and Youtube. *Brown Journal of World Affairs.* Vol. 16 (2), pp. 45-54

Wenz, J. (2015, February 10). This Cryptography Game Is Also a Navy Recruiting Tool. *Popular Mechanics.* Retrieved from: https://www.popularmechanics.com/military/a14020/this-crypto-game-is-a-navy-recruiting-tool/

Wheeler, K. (2014, November 26). Indigenous video game designer takes stand against Custer's Revenge. *CBC News.* Retrieved from: https://www.cbc.ca/news/indigenous/indigenous-video-game-designer-takes-stand-against-custer-s-revenge-1.2851104

Winkler, R., Nicas, J., & Fritz, B. (2017, February 14). Disney Severs Ties With YouTube Star PewDiePie After Anti-Semitic Posts. *The Wall Street Journal.* Retrieved from: https://www.wsj.com/articles/disney-severs-ties-with-youtube-star-pewdiepie-after-anti-semitic-posts-1487034533?mod=e2tw

Wyatt, R. (2020, December 8). 2020 is YouTube Gaming's biggest year, ever: 100B watch time hours. *Blog.Youtube.* Retrieved from: https://blog.youtube/news-and-events/youtube-gaming-2020/

Xiao, L. Y. (2023). Breaking Ban: Belgium's Ineffective Gambling Law Regulation of VideoGame Loot Boxes. *Collabra: Psychology,* 9(1). http://dx.doi.org/10.31219/osf.io/hnd7w

Yin-Poole, W. (2015, November 16). Sony responds to claim PS4 used for terrorist communications. *EuroGamer.* Retrieved from: https://www.eurogamer.net/sony-responds-to-claim-ps4-used-for-terrorist-communications

Zhang, X. (2020, March 6). The Evolution of Business Models in The Video-Game Industry. *EDHEC Business School.* Retrieved from: https://www.edhec.edu/en/news/evolution-business-models-video-game-industry

IN COLLABORATION WITH

LUND UNIVERSITY

Psychological Defence Research Institute

Psychological Defence Agency
Våxnäsgatan 10
SE–653 40 Karlstad
Mail: registrator@mpf.se
Phone: +46 10 183 70 00
www.mpf.se