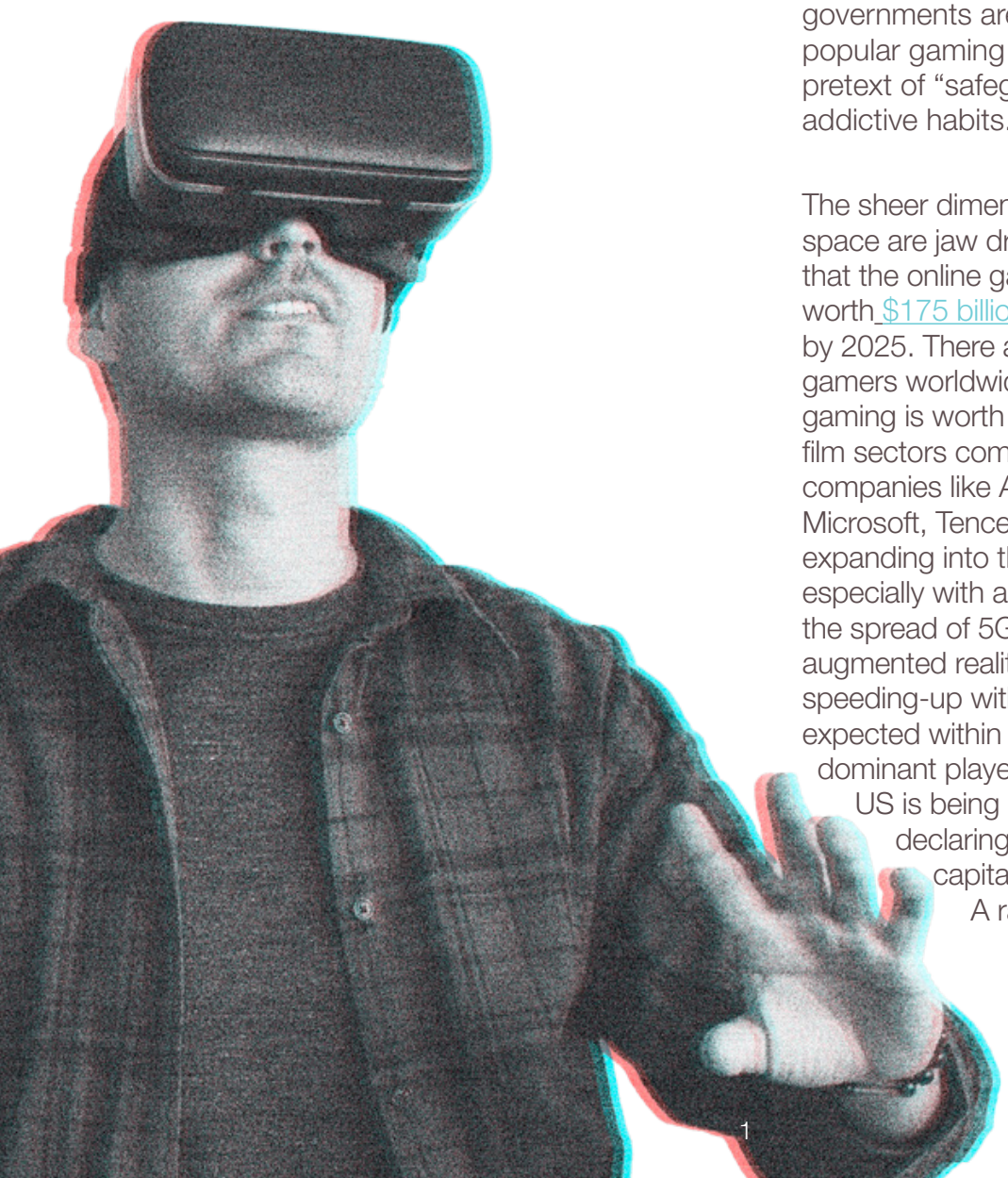
THE GREAT *(ONLINE)* GAME

JANUARY 2022

SecDev

THE GREAT *(ONLINE)* GAME



Online gaming is not just fun and games. To be sure, immersive gaming platforms are sites of playful cooperation for hundreds of millions of users. But they are also vehicles for selling products, sharing ideas, stealing secrets, radicalising users, and engaging in very real digital contestation. The astronomical popularity of multi-person online games is not lost on political actors. On the one side is a new generation of tech savvy politicians like Alexandria Ocasio-Cortez who are incorporating platforms like Twitch and Nintendo into their digital outreach strategies in order to woo prospective voters. On the other are pro-democracy advocates across Asia who are using games to set-up virtual protest sites where real world demonstrations are banned. Not surprisingly, a growing number of authoritarian and democratic governments are pushing back against popular gaming companies under the pretext of "safeguarding" young people from addictive habits.

The sheer dimensions of the digital gaming space are jaw dropping. Analysts estimate that the online game industry is currently worth $175 billion and that it will double by 2025. There are as many as 2.8 billion gamers worldwide which explains why gaming is worth more than the music and film sectors combined. Chinese and US companies like Apple, Activision, Google, Microsoft, Tencent and Zynga are rapidly expanding into the meta-gaming space, especially with advances in augmented reality, the spread of 5G and cloud computing. The augmented reality gaming sector is also speeding-up with over 200 million users expected within the next few years. Once the dominant player in the gaming space, the US is being outpaced by Asia, with China declaring its intent to become the capital of online gaming by 2025. A race is on for global online gaming supremacy.

The offline harms of online gaming

The explosive growth of gaming, especially since the onset of COVID19, is deepening concerns among researchers who study its long-term effects. Online games have long been associated with behavioral and physiological effects among adolescents and children. The risks associated with extensive play and health problems associated with prolonged play are linked to visual impairments, muscular injuries, obesity, diabetes and epileptic seizures. Social scientists have shown how video games can lead to pathologies and stunted development due to "screen time." Sociologists in particular have shown how online gaming is spreading cyber-bullying and heightening exposure to online predators, especially in virtual reality games. According to the Center for Countering Digital Hate, a violating incident occurs every few minutes on the virtual reality game, VRChat. These challenges will likely grow even more serious with the spread of so-called "haptic vests" that relay physical sensations to players. The "protection of healthy growth of minors" was one of the reasons, albeit arguably not the most important, behind China's decision to bar under-18 year old's from gaming on weekdays and to just three hours on weekends (a significant tightening on earlier restrictions set in 2019).

Online gaming is also a growing risk for adult players, many of whom are showing signs of addiction and gambling. This is especially the case in the metaverse since virtual reality creates an all-encompassing digital environment that stimulates a wider range of senses. The University of Nottingham's International Gaming Research Unit (IGRU) has studied the psychological and physiological effects of protracted gaming on older users. So-called "internet gaming disorder" (IGD) was recently proposed as a new mental disorder to be added to the Diagnostic and Statistical Manual (DSM) manual widely used by psychologists around the world. While an acknowledged problem, comparatively little action is being taken to prevent addictive gaming, the potentially dangerous ways adults interact with online games, and the on and offline harms that might arise.

The effects of online games extend beyond physical and psychological harms. A growing crop of online games and gaming communities are increasingly linked to the spread of extreme right groups. The problem is hardly new: it's been festering for years. The so-called "Gamergate" controversy of 2014 and 2015 is case in point. It

involved the targeting of female game developers and critics and acrimonious arguments over feminism, sexual harassment and journalist integrity. Gamergate is associated with the rise of what is now labelled the “alt right”. This helps explain why toxicity is often described as a feature of gaming culture, not a bug. These toxins are increasingly difficult to track in virtual reality games for the simple reason that toxic incidents transmitted simultaneously via headsets and chat messages occur in real time and are not always recorded.

While the majority of users are simply enjoying themselves, gaming platforms such as DLive, Steam and Roblox are connected to a range of violent pathologies that could just as easily translate from the online to the real world. In the UK, for example, far-right extremist groups are leveraging games and tournaments from Discord and Fortnite to Call of Duty and World of Warcraft to recruit young people despite guidelines prohibiting such behavior. A think tank, Tech Against Terrorism, has uncovered users being invited to reenact Anders Brievik’s 2011 terrorist attack in Norway or the 2019 mosque shootings in Christ Church. Users are provided with

everything from comprehensive bomb-making instructions to simulated vehicle attacks against protesters. The reality is that many gaming platforms have failed to design-in measures to deter abusive users and actions.

Online games also invariably lead to increased risk of exposure to privacy infringements, especially among younger users. One especially obvious concern is that children and adolescent players disclose personally identifiable information allowing cyber criminals to manipulate and access their online accounts and eventually commit fraud and identity theft. Other kinds of cyber-risks abound, including the intentional infection and manipulation of connected gaming devices as well as webcams, consoles, tablets and desktops. While most gaming companies urge users not to give away personal information, these warnings are frequently ignored, especially in faster-growing markets where digital literacy and a culture of privacy are underdeveloped.

A related consequence of expanding online gaming is malware, especially trojans, including viruses embedded in adware and “free” games. Advertising is common for most online games, and ad fraud is on the rise across mobile apps and online gaming platforms that require users to watch commercials before being allowed to play. At best, misleading ads can create friction and erode trust. At worst, these trojans can convert machines into larger botnets with consequential ripple effects. As ever, attribution is challenging, since some of these viruses may be hard to link to online games given delays intentionally designed-into the malware. The response to this challenge is typically more vigilance, due diligence and the use of multi-device cybers security software.

A vector for digital extremists and cybercriminals

The use of gaming platforms by violent extremists is drawing attention, but evidence of its pervasiveness is thin. The prospect of online games being exploited by terrorists and fanatics has long been a subject of speculation, to the point that it's been fictionalized in television shows. It is true that some extremist groups have even created their own "bespoke" video games or modified existing games to recruit and radicalize users. Notwithstanding riveting anecdotes of individual gamers being drawn into dark worlds of white supremacism and Nazi prison re-enactments, there is still comparatively few examples of gaming platforms being causally connected to real world fanaticism. To date, extremist use of gaming platforms seems mainly focused on reinforcing the views of already empathetic or radicalized players.

That said, the online game industry is being leveraged by state actors and increasingly targeted by established cybercriminals. Cyber security companies have detected a significant surge in attacks on gaming companies themselves from APTs, including APT41 targeting hundreds of gaming companies. Attackers are targeting source code, software code signing certificates, sensitive customer data and other items to repurpose and resell. The most prominent example of this was the recent attack on EA Sports, including theft of the company's source code. This came in the wake of ransomware attacks launched in November 2020 against CapCom, the makers of Resident Evil, and against CD Projekt Red (CDPR) in February 2020.

Despite growing awareness of data breaches, ransomware and phishing exploits, the threats appear to be accelerating rather than diminishing. A number of underground forums are auctioning off source code and data stolen from gaming companies - including the compromised accounts of millions of employees and clients. Credentials to the security networks of these companies are being sold on the DarkWeb, including usernames and passwords, and client facing resources. Breaches such as that reported against Amazon-owned gaming platform Twitch in October 2021 targeted source code, but likely also gathered up user information from some of its more than 51 million users. Not surprisingly, gamers are starting to take note. Queries for "how to delete Twitch" increased by over 700 percent after the incident was reported.

Grabbing the digital threat by the joystick

From west to east, governments and gaming companies are scrambling to deter online and offline risks. This includes building a stronger evidence base and identifying methods to counteract extremist use of online games. For example, the European Union's Radicalization Action Network Communications and Narratives working group (RAN C&N) has studied the issue since 2020. The Royal United Services Institutes Extremism and Gaming Research Network (RUSI EGRN) is another more recent collaboration that includes a wide array of primarily European violence prevention organizations. The latter's October 2021 State of Play report offers a powerful source of evidence related to gaming and violent extremism. Likening online games to a kind of "spiritual opium", China has tightened rules around gaming, including limiting screen-time, censoring content and encouraging more patriotic games.

Still, gaming industry participation in discussions about harms on their platforms is limited, and the industry is widely criticized for failing to manage risks to their customers. Gaming researchers like Daniel Kelley at the Anti-Defamation League (ADL) are vocal about the industry's general failure to effectively moderate and police their platforms. For the last three years, ADL has been conducting a yearly survey and publishing an industry report card that has shown an epidemic of hate and harassment in online games. ADL argues that these issues are finally being recognized as "systemic and repeated rather than episodic," and argues that the industry is overdue for a reckoning.

Embryonic gaming industry efforts to counter online hate and harassment provide a possible model for wider collaboration. There are early signs of progress around industry participation in research and healthy game design. The Fair Play Alliance (FPA) has attracted more than 200 gaming companies, including major global firms like Blizzard, EA, Roblox and EPIC. Among other things, they collaborated with ADL to produce a Disruption and Harms in Gaming Framework that provides a nuanced, realistic and authoritative taxonomy of online harms related to gaming. They also publish occasional white papers that provide practical, industry-focused advice on topics like content moderation and parental participation. Membership in FPA is open to any gaming company of any size. Evidence of impact is still comparatively thin. Whether these and other strategies work still amounts to a throw of the dice.

Navigating gaming 3.0 - identifying opportunity and managing risk

The online gaming space is undergoing a major acceleration in 2022. Facebook's rebranding as Meta in October 2021 marked a significant milestone in the transition towards web 3.0. Augmented and virtual reality together with ubiquitous mobile computing will continue to transform game space thrusting into the center of the consumer Internet as social media did a decade ago. Rather than watching from the sidelines, several other larger companies are already following suit.

These new immersive spaces will drive multiple forms of innovation in and outside the gaming sector. As with previous generations of gaming, they will generate new opportunities and risks. The next generation of gamers - Generation Z and especially Generation Alpha - are growing up with AI. Most of them already equate the Internet with social media and massively popular online games such as Minecraft and Roblox. As games become more sophisticated and accessible, the next 2 billion Internet users are likely to have their first encounter with cyberspace within the gaming space.

Even than in the case of social media, the immersive nature of gaming 3.0 will deepen debates in all societies about their potential digital harms and benefits. As TikTok's algorithms show, immersive platforms driven by AI open up new horizons capturing consumer behavior as well as shaping and influencing decisions. The defining interactive nature of game space means that decisions on what to buy, or what to think, will not be shaped on the basis of receiving a media product, but rather formed in interaction with it.

Keeping abreast of the dynamic growth in the gaming sector is critical for governments and corporations interested in harnessing market opportunities and mitigating the potential digital harms. SecDev actively monitors political, economic, social and technological trends and developments in online gaming. Our global risk practice tracks the evolution of gaming AI as well as implications of adoption across all major markets. We also keep abreast of the latest academic research on the impact of gaming on different demographic segments of society.

The emerging reality of the Metaverse calls for new, appropriate and ethical analysis and research. These include focus groups, interviews, direct interaction in gameplay and the use of statistical and machine-learning driven methods to bring state-of-the-art insights into the present and future of the game space environment. With more than 20 years proven track record and unprecedented access to a network of global researchers, SecDev leverages the full spectrum of research methods to design customized research portfolios and data feeds that capture market opportunities and quantify liabilities.

We provide our clients with a range of **white glove services** to assess and act on emerging opportunities.

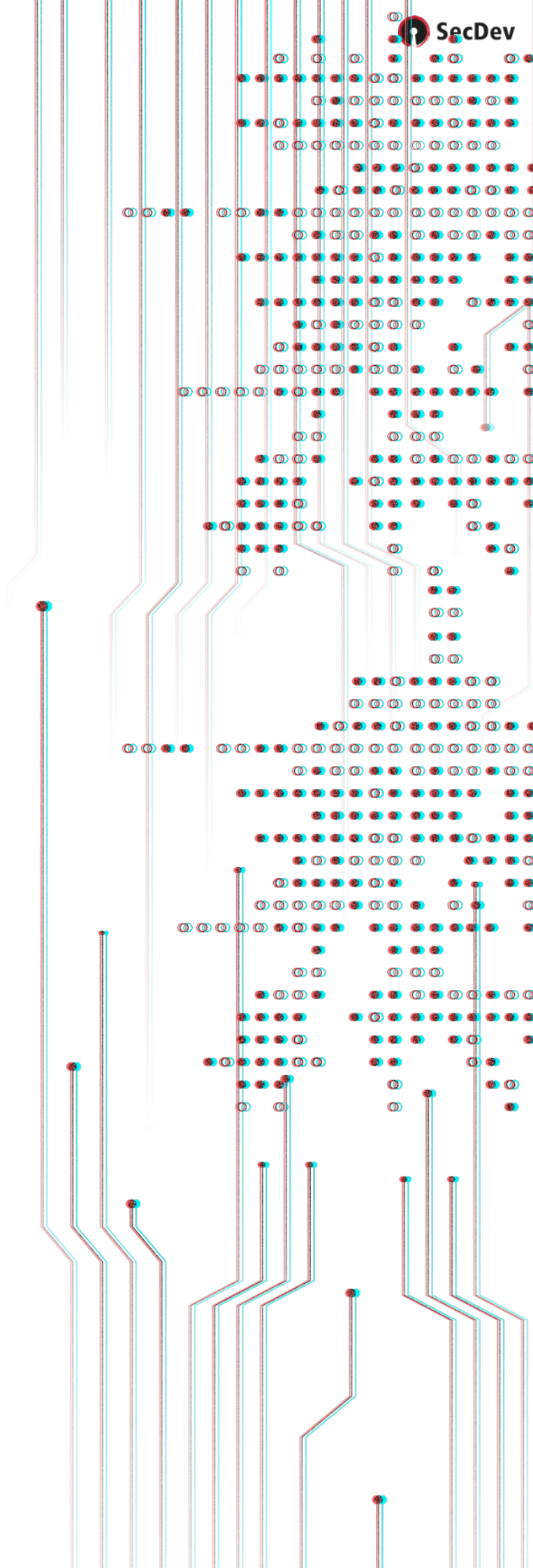
- **Discrete market studies, briefings and assessments** - that map opportunities and liabilities in specific verticals, geographic and linguistic markets.

- **Investigation and discovery** - to uncover hidden opportunities or investigate the causes of digital harms.

- **Simulations and Scenario planning** - to develop strategies for market entry, test ideas for product placement, shape public policy or to design and train in-house teams focused on future oriented analysis.

- **Data feeds and customized AI driven dashboards and visualizations** - to inform action and enhance situational awareness for C-suite, management, security, trust and safety, marketing and product development teams.

Whether your interest is in market entry or product promotion, or in minimizing liabilities through proactive public policy, SecDev's data-driven global expertise is there to navigate the complexities of the emerging Web 3.0 market.



About SecDev

SecDev is an agile research and innovation firm helping clients navigate digital-geopolitical, geospatial and geodigital risk. Our team of forecasters and data scientists support a wide range of clients including public sector, corporations and international organizations in meeting their need for timely, accurate decisions. We transform data into intelligence and identify opportunities to drive digital transformation. SecDev builds value through strategic foresight, data science on demand and intelligence as a service. We are global in scope, fluent in data collection and analytics, experienced in cutting edge technology and singularly results-oriented. We empower clients to make informed choices in a rapidly digitizing era.

SecDev

To learn more, visit **www.secdev.com**

Layout
Raphael Durão - STORMdesign.com.br