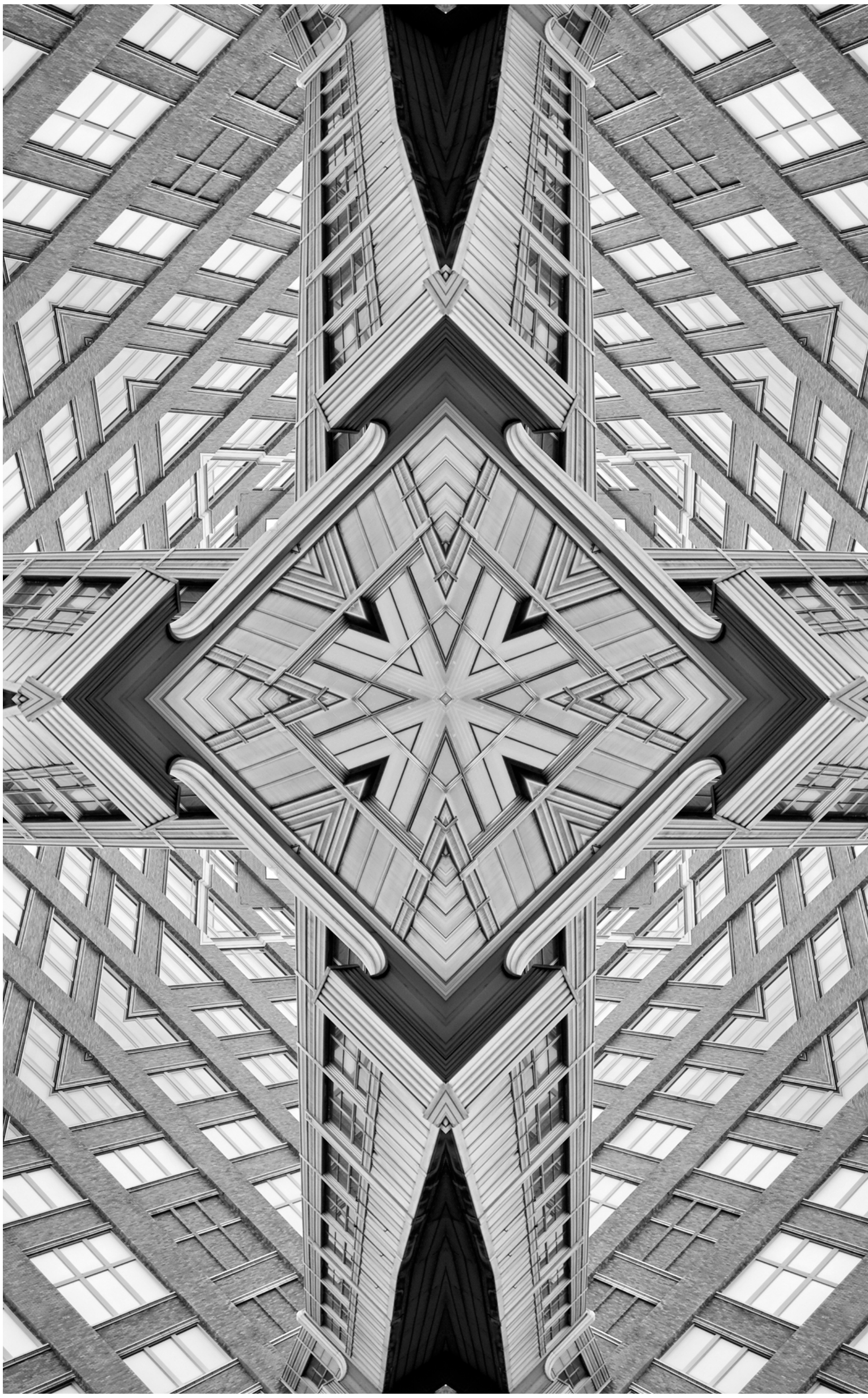
ORF OBSERVER RESEARCH FOUNDATION

Issue Brief

ISSUE NO. 684
JANUARY 2024



Cybersecurity Threats in Online Gaming: Learnings for India

Prateek Tripathi

Abstract

This brief examines the rapid growth of the global online gaming industry and the consequent increase in cyber threats. Issues such as microtransactions, money laundering, and predatory practices by developers can stymie the industry's growth potential if not addressed. Many countries' current gaming-focused regulatory frameworks do not cover these challenges and will need to be revised. India—a significant gaming market—must also consider making its online gaming policy more holistic by addressing the rampant cybersecurity threats.

Attribution: Prateek Tripathi, "Cybersecurity Threats in Online Gaming: Learnings for India," *ORF Issue Brief No. 684*, January 2024, Observer Research FoundAation.

Introduction

From the emergence of the coin-operated arcade game Pong in 1972 to the release of *Hogwarts Legacy*, an action role-playing video game, in 2023,[a] the gaming industry has come a long way.[1] Although video games are often stereotyped as being isolating and promoting antisocial behaviour,[2,3] the COVID-19 pandemic highlighted their ability to bring people together from different corners of the world.[4] Indeed, the gaming market grew by 26 percent between 2019 and 2021 amid the pandemic.[5] The industry's growth has also been driven by cloud and mobile platforms providing greater accessibility to video games, with players no longer needing expensive consoles and personal computers to access games. In 2022, mobile gaming accounted for nearly half of the industry's total value.[6] This has had an outsized influence in India, which recorded the largest number of mobile gamers worldwide in 2021-22 (about 507 million users),[7] amid increasing smartphone penetration due to affordable devices and data plans.

As of 2023, there are approximately 3.09 billion active video game players worldwide, and the number is expected to reach 3.32 billion by 2024.[8] The global gaming industry was worth over US$227 billion in 2022, more than the American film and music industries combined,[9] and is further projected to grow to US$312 billion by 2027.[10] Revenues will continue to increase, primarily driven by higher investments in in-app advertising. Advertising revenue is projected to nearly double between 2022 and 2027, crossing US$100 billion by 2025.[11]

Though the gaming market has thus far been dominated by China and the US, future growth in the sector is expected to come from emerging economies with growing populations. It is expected to expand the fastest in Türkiye, with an average annual growth rate of 24.1 percent between 2021 and 2026, followed by Pakistan and India, with an expansion of about 21.9 percent and 18.3 percent, respectively.[12]

However, as the online gaming industry has grown in popularity, there has also been a rise in cyberattacks on gaming platforms. For instance, there was a 167-percent year-on-year increase in web application[b] attacks in 2021.[13] In 2022, the gaming industry became the biggest target of distributed denial-of-service (DDoS) attacks, accounting for about 37 percent of all such incidents.[14] Account

[a] *Pong* is one of the earliest video games and played a pioneering role in establishing the industry. *Hogwarts Legacy* is part of the popular *Harry Potter* franchise and the largest-selling video game in 2023.

[b] A web application is a software that runs in web browsers. It enables a convenient and secure exchange of information, and delivery of services for customers. Common website features like shopping carts, instant messaging, and social media newsfeeds are some examples of web applications. Games accessible via websites without prior installation are also web applications.

Introduction

takeovers, cheating mods,[c] credit card theft, and fraud are the most common forms of cyber threats on gaming platforms. Gaming companies have also been victims of intellectual property (IP) theft, credential theft, and ransomware (such as the recent hack of Take-Two Interactive and the subsequent public leak of *Grand Theft Auto 6*[15]). Additionally, a significant cybersecurity incident occurred in March 2023, when classified US intelligence documents were leaked on a video game chat server, in what some described as the worst Pentagon leak in years.[16]

The Indian gaming industry is a significant component of the global market. In 2023, its revenues reached US$3.1 billion, up US$500 million from the previous year, and it is expected to grow at a compound annual growth rate of 20 percent in the future.[17] At the same time, Indian gamers have also encountered cyber threats, with 75 percent of gamers surveyed in the country in a 2021 report stating they experienced a cyberattack on their gaming account.[18]

This issue brief examines the cybersecurity threats posed by online gaming and what steps countries, including India, can take to mitigate these threats.

[c] A mod or modification is an alteration of a game created by players instead of developers. A cheating mod is a mod that has not been approved by the game developer and is used by players to gain an illegitimate advantage over others in online games.

Cyber Threats in Online Gaming: Types and Instances

The online gaming industry has become a prime target for various cyberattacks. Some of the most common forms include:

- **DDoS Attacks***:* DDoS attacks are the most common form of web application attacks. These are attacks where the attacker floods web servers with false requests to overload them. This overwhelms regular server traffic and can cause servers to respond more slowly or crash altogether. DDoS attacks usually target websites but can also be used to target online gaming servers or even individual gamers through their IP address which in turn can be acquired through malware. The motivations behind these attacks are varied, but they are usually done to make the user's online gaming system slow and unplayable, with the intent to gain a competitive edge.

- **Phishing Attacks and Personally Identifiable Information Leaks***:* Phishing is the most common form of an online social engineering attack,[d] by deceiving, manipulating, or pressuring individuals into divulging sensitive personal information. The attacker typically poses as a trusted individual or corporation requesting personal information like credit card and bank account details or login credentials. Once acquired, these can be misused or sold. If a gamer is in the habit of reusing passwords, gaming account details can also be used for credential stuffing[e] on other websites to steal more valuable information.

  Personally identifiable information leaks refer to cyberattacks where users' valuable personal information is collected. This data may be acquired via phishing attacks, hacking company databases, or using developer errors to expose data. This information can be used for identity theft, account takeovers, swatting,[f] or doxing.[g]

[d] A social engineering attack uses manipulation techniques that exploit human error to access private information, expose data, and spread malware.

[e] Credential stuffing refers to a type of cyberattack in which usernames and passwords stolen from one source or organisation are used to access accounts at another source or organisation.

[f] Swatting refers to a harassment technique that involves generating an emergency law enforcement response against a target individual under false pretences.

[g] Doxing is a cyberattack in which the attacker posts an individual's personal details online, to humiliate, intimidate, or blackmail.

- **Malware:** Malware or malicious software refers to intrusive software that is intentionally designed to cause damage to or extract personal information from computers. It is an umbrella term for various online threats, such as adware, spyware, ransomware, and viruses. When users try to find cheaper or free versions of games, they may risk downloading malware or viruses. This can also happen while trying to access cheats or purchasing in-game content through third-party sellers. Hackers are known to infect legitimate games with malware by exploiting security gaps.[19]

There have recently been a few significant instances of cybersecurity attacks emanating from the online gaming sector.

- ### Classified US defence document leak on discord

In early 2023, several highly classified documents from the US defence department, including some marked 'top secret', were leaked on a Discord[h] server dedicated to the popular video game *Minecraft*.[i] This data later found its way to social media platforms like X (formerly Twitter) and Telegram.[20]

Netherlands-based open-source intelligence research firm Bellingcat tracked the leaks, reporting that ten documents were posted on a Discord server called 'Minecraft Earth Map' in March.[21] The documents contained sensitive information related to the ongoing Ukraine-Russia war (such as Ukraine's status in its ongoing conflict with Russia, potential problems with Ukrainian ammunition supplies, and the losses sustained by the Russian military), and also indicated that the US had been spying on its allies, particularly Israel and South Korea. The motivation behind the leaks remains unclear, but Bellingcat reported that it seems to have originated from an online spat between two gamers over Russia's war in Ukraine. One of the users, a 21-year-old US National Guard airman, seems to have posted the classified documents to win the debate. The leaks reportedly originally began in February 2022 in a Discord group called 'Thug Shakers Central' created by Teixeira, and later spread to other Discord servers and social media platforms.[22]

[h] Discord is an application used by gamers to chat, communicate, and stream video games. This is done in private, invitation-only servers, which are usually dedicated to a particular game.

[i] Minecraft is a sandbox game that has become one of the best-selling video games ever with over 238 million copies sold as of 2023. It has over 140 million monthly active players. A sandbox game is a type of video game that allows players to have a high degree of freedom to explore and interact with the game world in a nonlinear fashion.

Incidentally, this was not the first instance of classified information being leaked by the gaming community. In 2022, forums connected to *War Thunder*, a combat video game focused on military vehicles, had leaked weapon schematics, such as details on the F-16 fighter jet and the UK's Challenger 2 tanks.[23]

These instances show that gaming forums and applications are often used to divulge potentially classified information. Governments and policymakers around the world must have a serious conversation about why this happens and where these leaks originate from. One possible cause could be the US military's recent attempts to identify and engage Gen Z recruits by using online gaming platforms like Discord. The platform already runs a 17,000-member server for service members to discuss first-person shooter games and participate in the so-called 'Army of Tomorrow'[24,25] as part of the Army Recruiting Command's *Army e-Sports Programme*, which is designed to unite the Army and general population through a shared passion for gaming.

- **Cyberattacks on gaming companies**

Gaming companies have also been the focus of cyberattacks on several occasions, most attributed to phishing or online social engineering attacks. In September 2022, Rockstar Games, creator of the multi-billion-dollar gaming franchise *Grand Theft Auto*, was hacked, and about 50 minutes of footage from its upcoming game *Grand Theft Auto 6* was leaked.[26] The attack was conducted by a 17-year-old from the UK, known by the pseudonym 'Teapot', who tried to hold the company hostage over the game's source code. He was later also found to be responsible for an Uber data breach. In both cases, messaging app *Slack* was used to conduct a phishing attack and deceive company employees into handing over their login credentials by Teapot, who was pretending to be a company IT worker.

In January 2023, another prolific video game company, *Riot Games*, fell victim to an online social engineering attack.[27] While the company claimed that no user data had been compromised, the source codes of some of its popular games, such as *League of Legends* and *Teamfight Tactics*, were stolen and the hackers allegedly asked for a US$10 million payout.

The FBI received more than 323,000 complaints of social engineering attacks across all platforms in 2021, which is about three times more than in 2019, with the hackers stealing roughly US$2.4 billion in the process.[28]

- **In-game currency, gambling laws, and money laundering**

Developers have sought new ways to monetise the growing popularity of online gaming. This has led to the creation of virtual or in-game currencies that can be purchased using real money, usually via credit cards. The virtual currency can be used to conduct 'micro-transactions'[j] or purchase 'loot boxes'.[k] Such currency is increasingly prevalent in both mobile and console/PC games, particularly free-to-play games, and generates huge amounts of revenue.

In-game currency and loot boxes have generated much controversy for becoming a form of predatory monetisation by developers, particularly targeting minor or novice players. Several countries have banned the use of in-game currency and loot boxes, considering them a type of online gambling. For instance, in 2018, the Belgian government banned the purchase of 'FIFA points' (an in-game currency) in the online FIFA games made by Electronic Arts (one of the biggest video game developers worldwide).[29] FIFA points could be used to purchase card packs (a kind of loot box) to get a randomised selection of players or items. The Belgian Gambling Commission declared that loot boxes essentially amount to gambling since they are games of chance. In February 2023, Austria declared FIFA packs as "illegal gambling."[30] The Dutch government has also recently announced its intention to completely ban loot boxes in all games.[31]

Another outcome of microtransactions and the increasing value of in-game items has been the generation of an additional avenue for money laundering. The virtual economy in video games has become a flourishing market, with items that can cost up to millions of dollars,[32] making them a prime target for money launderers. Gaming marketplaces provided by games like *Call of Duty* are often overcrowded and hard to monitor. Launderers can purchase in-game currency or items using a prepaid, single-use credit card, and subsequently put these up for sale on third-party websites where they are purchased by enthusiastic gamers, usually via cryptocurrency, with the seller receiving his payment immediately. This transaction leaves behind no trace of identity or income source. In 2019, video game developer *Valve* had to halt online transactions for its popular game *Counter-Strike: Global Offensive* after noting that 90 percent of its microtransactions resulted from money laundering practices.[33]

[j] Small in-game transactions that unlock specific content or features. The content can be purely cosmetic, like outfits and shaders, or items affecting gameplay, like experience boosts and weapons.

[k] A variant of a microtransaction. Players can purchase a virtual item (or a 'loot box'), which contains a randomised selection of virtual items. The catch is that the player does not know what they will get in advance.

In May 2023, India's Enforcement Directorate managed to track and conduct a nationwide crackdown on foreign-registered online gaming companies suspected of laundering INR 40 billion (US$480 million).[34] These companies were registered in tax havens like Curaçao, Malta, and Cyprus, and were linked to Indian bank accounts opened in the names of proxy persons with no links to online gaming activity. They could only be tracked since they violated the provisions of the Foreign Exchange Management Act,[35] which does not allow remittances out of income from racing, riding, or any other hobby. This would not have been the case had the laundering occurred via virtual currencies.

- **Predatory practices by videogame developers and dark patterns**

The potential of video games to generate massive revenues has given rise to predatory and unethical practices by the gaming industry. Game developers have increasingly used microtransactions and 'dark patterns' to target users. Dark patterns refer to deceptive designs used in websites and applications to trick customers into taking unintended actions, such as purchasing items, signing up for services or agreeing to recurring subscriptions.

In December 2022, Epic Games, creator of the popular game *Fortnite*, had to pay US$520 million in relief after the US Federal Trade Commission (FTC) charged it for violating the Children's Online Privacy Protection Act (COPPA) and using dark patterns to dupe millions of players into making unintentional purchases.[36,37] Epic allegedly violated the COPPA rule by collecting personal information from children under the age of 13 without notifying their parents or obtaining their consent. It was also accused of enabling real-time voice and text chat for children by default, which led to several instances of harassment and bullying. Until 2018, Epic also allowed children to purchase the in-game currency (V-bucks) without obtaining parental or card-holder consent. The US FTC has brought similar complaints against companies such as Apple, Amazon, and Google for billing consumers millions of dollars for in-game content purchased by children without parental authority.[38]

The Global Regulatory Scenario

Many countries have established regulatory frameworks pertaining to online gaming, but these are lopsided, focusing primarily on gambling and sidestepping many of the more common cyber threats. As such, there is an urgent need to revamp these laws to tackle the more rampant cybersecurity threats plaguing the gaming industry.

- In the European Union, online gambling and gaming are governed by the European Gaming and Betting Association (EGBA).[39] Online gaming companies associated with the EGBA abide by a large set of industry standards designed to complement the numerous licencing guidelines they already adhere to in European countries. Some of the objectives laid out by the EGBA include the prevention of underage gambling, safeguarding customer privacy, fair and responsible gaming, and the prevention of money laundering.

- In the UK, online gaming comes under the jurisdiction of the 2005 Gambling Act.[40] It mainly contains rules and regulations for online gambling on gaming platforms. For instance, social gaming applications and sites can offer real money prizes, provided they are purely skills-based. Gambling and casino games can circumvent these regulations by offering prizes in virtual currency and thus do not fall under the purview of the Act.

- In the US, online gaming is governed by the 1961 Interstate Wire Act, better known as the Federal Wire Act, and the Unlawful Internet Gambling Enforcement Act.[41,42] Like the UK, these acts mostly regulate online gambling and sports betting. Social gaming and video games are not a focal point of these laws.

- Gambling is strictly forbidden under Islamic law and, as such, is restricted in many West Asian countries. For instance, in the UAE, the Telecommunications Regulatory Authority has implemented the Internet Access Management Regulatory Policy, which requires internet service providers to block access to websites providing illegal content, such as gambling.[43] However, notably, there are no laws specific to online gaming. Consequently, microtransactions and loot boxes are legal in the country.

- India notified new rules for online gaming in April 2023.[44] These rules are meant to amend some of the provisions of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The amendments define an online game as one "that is offered on the internet and is accessible by a user through a computer resource if he makes a deposit with the expectation of earning winnings." The rules also detail which online games are permissible: online real money games registered with self-regulatory organisations (SROs),[i] and games not involving real money. The new rules ban all online games involving betting and wagering while laying out provisions for establishing three SROs entrusted with the responsibility of approving games that fall under the operational guidelines set out by them. They also define online gaming intermediaries as "any intermediary that enables the users of its computer resource to access one or more online games," and detail their obligations. Know-your-customer norms, parental consent, and grievance redressal mechanisms are some further issues that have been addressed by the new rules.

> "Although some countries have established regulatory frameworks pertaining to online gaming, these are often lopsided, focusing primarily on gambling and sidestepping many of the more common cyber threats."

[i] SROs are envisioned to be groups of industry representatives, educationists, and other experts responsible for deciding which online games are permissible.

Although India has notified new rules on online gaming, its current policy framework cannot contend with the issues threatening this sector. The existing law only focuses on games involving real money and wagering, drastically limiting their scope. Most online games are riddled with microtransactions and, hence, can easily circumvent these rules. Additionally, games can completely bypass these laws just by offering prizes in virtual currency. Moreover, there is no mention of loot boxes in these rules, meaning they remain completely legitimate. Similarly, purchasing FIFA points remains legal in India despite many countries banning their use. This also indicates that the gaming laws will have no bearing on money laundering conducted through online gaming since these are carried out via virtual currencies and purchases of in-game items, which Indian laws do not address. The absence of mention of loot boxes and microtransactions in the new Indian gaming laws is a significant oversight that needs to be addressed immediately. There also needs to be a discussion on whether allowing loot boxes in video games amounts to gambling and what kind of impact it has on players, particularly children and minor users. Global experiences with this particular aspect of regulating online gaming can provide guidance to Indian lawmakers.

The issue of money laundering via video games also requires a deeper engagement since tracing virtual currency transactions is extremely difficult. The imposition of a 28 percent tax on online gaming from October 2023 onwards appears to be an attempt to address this issue,[45] but it risks hampering the growth of the burgeoning industry.

Another aspect that needs inclusion in Indian laws is the leaking of sensitive information via gaming forums and applications such as Twitch[m] and Discord. Content moderation on these applications and forums is also an issue that should be addressed since they have often been used as gambling dens, distribution hubs for pornography and illicit content, and other nefarious activities. International collaboration, perhaps coordinated by the International Association of Gaming Regulators, would be beneficial.[46]

[m] Twitch is a live-streaming service with a particular emphasis on video games. It is also used for streaming sports, music, and other creative content.

Recommendations

India should consider the following to make its online gaming laws and policies more holistic:

- Incorporate the issue of microtransactions and loot boxes into existing gaming laws. While an outright ban on games employing these might be construed to be extreme by both developers and consumers, there are milder steps that can be taken. For instance, the Indian government can devise its own rating system, similar to the Entertainment Software Rating Board and the Pan European Games Information systems,[n] and rate these games as 'mature' so players under the age of 18 cannot access them.

- Empower agencies such as the Competition Commission of India to investigate online gaming from the viewpoint of consumer interest protection to check the predatory practices of video game developers. This would also go a long way in ensuring the orderly development of the online gaming market in India.

- To tackle the issue of money laundering via video games, consider including virtual currency investments into the Liberalised Remittance Scheme,[47] under which Indian citizens residing in the country can repatriate up to US$250,000 per year abroad for a disclosed purpose. Allowing Indians to use this overall limit for purposes like investment in virtual currencies would bring gaming purchases under the radar of trackable transactions. This would also allow better monitoring of such transactions by linking them to user bank profiles to identify unscrupulous and fraudulent users.

- The recent US intelligence leaks should lead to discussions and debates in India and other countries on regulating applications like Discord, while closely monitoring any online initiatives where the military engages with the general population, especially when it involves officials with access to sensitive information. There is also a need to promote safe gaming practices among players. Most cyber threats at an individual level are simply a consequence of ignorance. Gamers need to be educated on the kind of cyberattacks they can encounter and how to handle them. For instance, something as simple as using a virtual private network (VPN) can eliminate many potential cyber threats.

[n] Entertainment Software Rating Board (applicable in the US, Canada, Mexico) and the Pan European Games Information (applicable in the UK and many European countries) are ratings systems that provide information about the contents of a game so users can make informed choices regarding which games are suitable.

Conclusion

The online gaming community has grown exponentially in recent decades and is poised for substantial further growth. In addition to uniting millions of people worldwide—and despite the security threats this presents—gaming platforms also have great potential for good. For instance, in 2021, the Z event, a charity event hosted on Twitch, raised about US$11.5 million for Action Against Hunger (a global organisation focused on ending world hunger).[48] Discord also hosts several charity servers, such as the 'Military and Veteran Gamers Charity' server that offers mental health peer support programmes.[49] Notably, online gaming also provided people with some much-needed relief during the pandemic by acting as a means to interact and engage with like-minded individuals from within the isolating confines of their homes.[50]

Still, governments and policymakers worldwide must pay attention to the escalation in nefarious activities—both in absolute numbers and types—in online games, and the larger societal threats they present. Online gaming is one of the fastest-growing sectors in the global entertainment and media industry and provides a powerful avenue to unite people worldwide. As such, it is imperative to ensure the industry grows safely and responsibly for the good of users and developers. India, which is poised to see significant growth in its gaming market, will also need to develop a more holistic online gaming policy.

Prateek Tripathi *is a Research Assistant at ORF's Centre For Security Strategy and Technology.*

Endnotes

1 Adrian Willings, "Video games through the ages: How games have changed over time," *Pocket-lint,* February 22, 2023, https://www.pocket-lint.com/games/news/149572-then-vs-now-video-games-through-the-decades/

2 Nicholas Taylor, Jennifer Jenson, Suzanne de Castell and Barry Dilouya, "Public Displays of Play: Studying Online Games in Physical Settings," *Journal of Computer-Mediated Communication*, Volume 19, Issue 4, 763–779, July 1, 2014, https://doi.org/10.1111/jcc4.12054

3 Rachel Kowert and Linda K. Kaye, "Video Games Are Not Socially Isolating," in *Video Game Influences on Aggression, Cognition, and Attention* (Springer, Cham., 2018), 185-195, https://doi.org/10.1007/978-3-319-95495-0_15

4 Bartosz Skwarczek, "How The Gaming Industry Has Leveled Up During The Pandemic," *Forbes,* June 17, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/06/17/how-the-gaming-industry-has-leveled-up-during-the-pandemic/

5 Simon Read, "Gaming is booming and is expected to keep growing," *World Economic Forum,* July 28, 2022, https://www.forbes.com/sites/forbestechcouncil/2021/06/17/how-the-gaming-industry-has-leveled-up-during-the-pandemic/

6 Andrea Knezovic, "200+ Mobile Games Statistics: Market Report [2023]," *Udonis*, April 12, 2023, https://www.blog.udonis.co/mobile-marketing/mobile-games/mobile-gaming-statistics

7 Donita Jose, "507 mn: India records largest pool of mobile gamers, pips China, America," *The Times of India,* November 5, 2022, https://timesofindia.indiatimes.com/city/hyderabad/507-mn-india-records-largest-pool-of-mobile-gamers-pips-china-america/articleshow/95310336.cms

8 Josh Howarth, "How Many Gamers Are There?" *Exploding Topics,* January 18, 2023, https://explodingtopics.com/blog/number-of-gamers

9 PricewaterhouseCoopers International Limited, *Perspectives from the Global Entertainment & Media Outlook 2023-2027*, June 21, 2023, https://www.pwc.com/gx/en/industries/tmt/media/outlook/insights-and-perspectives.html

10 PwC, *Perspectives from the Global Entertainment & Media Outlook 2023-2027*

11 PwC, *Perspectives from the Global Entertainment & Media Outlook 2023-2027*

12 PwC, *Perspectives from the Global Entertainment & Media Outlook 2023-2027*

13 Jonathan Reed, "Cyberattacks against gamers continue beyond 167% increase," *SecurityIntelligence,* April 5, 2023, https://securityintelligence.com/news/cyberattacks-against-gamers-increase-167-percent/

14 "Akamai Research Shows Attacks On Gaming Companies Have More Than Doubled Over Past Year," *Akamai,* August 4, 2022, https://www.akamai.com/newsroom/press-release/akamai-research-shows-attacks-on-gaming-companies-more-than-doubled-over-past-year

Endnotes

15 Keza Macdonald, Keith Stuart and Alex Hern, ”Grand Theft Auto 6 leak: who hacked Rockstar and what was stolen?” *The Guardian,* September 19, 2022, https://www.theguardian.com/games/2022/sep/19/grand-theft-auto-6-leak-who-hacked-rockstar-and-what-was-stolen

16 Jake Epstein, ”The worst Pentagon leak in years may have started in a gamer chatroom, where people weirdly keep posting classified documents trying to win arguments on the internet,” *Business Insider India,* April 12, 2023, https://www.businessinsider.in/international/news/the-worst-pentagon-leak-in-years-may-have-started-in-a-gamer-chatroom-where-people-weirdly-keep-posting-classified-documents-trying-to-win-argume-nts-on-the-internet/articleshow/99442978.cms

17 “Indian gaming industry poised for strong growth: projected to reach $7.5 Bn by FY28,” *Lumikai,* November 2, 2023, https://www.lumikai.com/post/indian-gaming-industry-poised-for-strong-growth-projected-to-reach-7-5-bn-by-fy28

18 NortonLifeLock, *2021 Norton Cyber Safety Insights Report: Special Release – Gaming & Cybercrime*, 2021, https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report-special-release-gaming-and-cybercrime/

19 Miriam Cihodariu, ”Cybersecurity for Gamers 101: Gaming Malware and Online Risks,” *Heimdal,* September 28, 2023, https://heimdalsecurity.com/blog/cybersecurity-for-gamers-101-malware-risks/

20 Chas Danner, “What Secrets Are in the Leaked Pentagon Documents- and Who Leaked Them?” *Intelligencer,* May 14, 2023, https://nymag.com/intelligencer/article/leaked-pentagon-documents-what-we-know.html

21 Epstein, “The worst Pentagon leak in years may have started in a gamer chatroom, where people weirdly keep posting classified documents trying to win arguments on the internet”

22 Danner, ”What Secrets Are in the Leaked Pentagon Documents- and Who Leaked Them?”

23 Epstein, “The worst Pentagon leak in years may have started in a gamer chatroom, where people weirdly keep posting classified documents trying to win arguments on the internet”

24 Vivek Mishra and Sameer Patil, “Pentagon Leaks: Heralding A New Counterintelligence Era,” *Observer Research Foundation,* April 25, 2023, https://www.orfonline.org/expert-speak/pentagon-leaks-heralding-a-new-counterintelligence-era/

25 Devon L., “Elite gaming: Army engages youth in esports,” *U.S. Army,* October 8, 2019, https://www.army.mil/article/224839/elite_gaming_army_engages_youth_in_esports

26 MacDonald et al., “Grand Theft Auto 6 leak: who hacked Rockstar and what was stolen?”

27 Arghanshu Bose, “Riot Games cyber attack: Hackers steal game source codes, demand ransom,” *The Times of India,* January 25, 2023, https://timesofindia.indiatimes.com/

gadgets-news/riot-games-cyber-attack-hackers-steal-game-source-codes-demand-ransom/articleshow/97319750.cms

[28] Brian Bushard, "Alleged Teenage 'TeaPot' Uber Hacker Arrested In England ," *Forbes*, September 23, 2022, https://www.forbes.com/sites/brianbushard/2022/09/23/alleged-teenage-teapot-uber-hacker-arrested-in-england/

[29] Tom Gerken, "Video game loot boxes declared illegal under Belgium gambling laws," *BBC*, April 26, 2018, https://www.bbc.com/news/technology-43906306

[30] Marco Wutz, "FIFA Ultimate Team packs are "illegal gambling," Austrian court rules," *Video Games on Sports Illustrated,* March 6, 2023, https://videogames.si.com/news/fifa-lootboxes-illegal-gambling-fut-packs-austria

[31] Evgeny Obedkov, "Netherlands plans to impose complete ban on loot boxes in video games," *Game World Observer,* July 4, 2023, https://gameworldobserver.com/2023/07/04/netherlands-loot-boxes-ban-video-games

[32] Josh Ye, "Man sues NetEase after his friend sells a US$1.4 million game character for US$500," *South China Morning Post,* November 21, 2019, https://www.scmp.com/abacus/news-bites/article/3038799/man-sues-netease-after-his-friend-sells-us14-million-game

[33] "Video Games: A Gateway To Online Money Laundering," *Financial Crime Academy,* October 18, 2023, https://financialcrimeacademy.org/video-games-a-gateway-to-online-money-laundering/

[34] "ED cracks down on offshore registered online gaming companies," *The Hindu Business Line,* May 24, 2023, https://www.thehindubusinessline.com/news/ed-crackdown-against-offshore-registered-online-gaming-companies-sniffs-laundering-of-4000-crore/article66889596.ece

[35] "Foreign Exchange Management Act, 1999," Income Tax Department, Ministry of Finance, Government of India, https://incometaxindia.gov.in/pages/acts/foreign-exchange-management-act.aspx

[36] Natasha Singer, "Epic Games to Pay $520 Million Over Children's Privacy and Trickery Charges," *The New York Times,* December 19, 2022, https://www.nytimes.com/2022/12/19/business/ftc-epic-games-settlement.html

[37] "Children's Online Privacy Protection Rule ("COPPA")," Federal Trade Commission, https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

[38] "Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges," Federal Trade Commission, December 19, 2022, https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations

Endnotes

39 European Gaming and Betting Association, https://www.egba.eu/

40 "Gambling Act 2005," Legislation.gov.uk, https://www.legislation.gov.uk/ukpga/2005/19/contents

41 "The Federal Wire Act Law Of 1961," *Gamblinglaws.org*, https://www.gamblinglaws.org/us/federal-wire-act/

42 "Unlawful Internet Gambling Enforcement Act," Federal Trade Commission, https://www.ftc.gov/legal-library/browse/statutes/unlawful-internet-gambling-enforcement-act

43 "Gaming and Gambling in UAE," *Rasma Legal*, October 20, 2022, https://rasmalegal.com/gaming-and-gambling-in-uae/

44 Ministry of Electronics and Information Technology, Government of India, April 6, 2023, https://www.meity.gov.in/writereaddata/files/Draft%20notification%20for%20amendment%20to%20IT%20Rules%202021%20for%20Online%20Gaming.pdf

45 Ministry of Finance, Government of India, August 2,2023, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1945208

46 International Association of Gaming Regulators, https://iagr.org/

47 "Liberalised Remittance Scheme," The Reserve Bank of India, April 6, 2023, https://www.rbi.org.in/commonperson/English/Scripts/FAQs.aspx?Id=1834

48 Nana Akosua Frimpong, "The Live Stream Event Raising Millions For Charity," *The Fifth Agency*, October 14, 2022, https://thefifthagency.com/trends/trendsetters-the-live-stream-event-raising-millions-for-charity/

49 "Military & Veteran Gamer Charity," *Discord*, https://discord.me/mvgcharity

50 Jin Yang, Ruoxu Wang, Amy Cook and Rhema Fuller, "Gaming during the COVID-19 pandemic: Examining its effect on loneliness & motivation, playing and gratification differences between competitive and recreational gamers," *Telematics and Informatics Reports*, Volume 11, 2023, https://doi.org/10.1016/j.teler.2023.100093

Images used in this paper are from Getty Images/Busà Photography.

ORF OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org