Turkish Online Journal of Qualitative Inquiry (TOJQI)

Volume 12, Issue 8, July 2021: 966-981

Contouring E–Doping: A Menace to Sportsmanship in Esports

Mr Subhrajit Chanda [a], Mr Tarun[b], Prof. Shaun Star [c]

[a] Assistant Lecturer, Jindal Global Law School, O.P. Jindal Global University, Sonipat, Haryana, India & PhD Candidate, GD Goenka School of Law, GD Goenka University, Gurugram, India.

[b] Assistant Professor (Research) at Gujarat National Law University (GNLU), Gandhinagar, India.

[c] Associate Professor and Associate Dean, Jindal Global Law School, O.P. Jindal Global University, Sonipat, Haryana, India

ABSTRACT: With the increase in the popularity and a promising revenue model of esports, the issue of e-doping has emerged. Some esports athletes may desire to deliver an outstanding performance to get an advantage over other competitors with the help of 'cheat software'. The paper explores various forms of e-doping such as disruption of live streams, attacking serversand discusses how these methods are a challenge to the spirit of fair play.

E-doping can take two forms: the use of hardware of software hacks to gain an unfair advantage, or the use of performance enhancing substances. To curb the menace of e-doping, different esports associations have used anti-cheating software such as*Value Anti-Cheat* (VAC), which monitors and tracks the movement of the player's input devices, by which a player could manipulate their moves. The establishment of the International Esports Federation (IESF) and the Esports Integrity Coalition (ESIC) have seen some progress in the regulation of integrity issues in esports.

Following the public admission of Kory "Semphis" Friesen in 2015, of using Adderall during a tournament of Counter Strike, ESL (an esports company) collaborated with the World Anti-Doping Agency (WADA) to develop the first anti-doping policy. Unfortunately, the implementation of this policy has not been effective as it could be, due to non-cooperation from different esports companies. In addition, this policy focuses on the use of banned substances, rather than other forms of in-game cheating. Consequently, the authors recommend reforms to e-doping policies. In addition, the authors further the debate about the importance of an improved governance structure which will assist the stakeholders to tackle the menace of e-doping, thereby promoting the principles of fair competition.

KEYWORDS: Gaming, Performance Enhancement, Anti-cheat, e-doping, esports,

1. INTRODUCTION

Esports has seen a massive rise in popularity in recent times. The term refers to the "*activity of playing computer games against other people on the internet, often for money, and often watched by other people using the internet, sometimes at special[ly] organised events*" (**Cambridge Dictionary, 2021**). Recently, online gaming has evolved from a leisure activity to a professional competitive environment with international organisations setting up worldwide tournaments. Live streaming of video games on platforms such as YouTube and Twitch has given the popularity of esports a significant push (**Hamari&Sjöblo, 2017**).This has helped bring spectators to esports, which was previously rare, and it has paved the way for individuals to become professional gamers and monetise their participation as gamers. The late 2000s saw a significant rise in popularity in multiplayer video game tournaments, with different gaming companies developing games with the scope of conducting such tournaments. The popularity of online multiplayer games skyrocketed, and currently, it is the driving force behind PC sales of 2.2 billion dollars (**Nalli, 2019**). The first games that gave rise to the popularity of multiplayer competitive gaming emerged in the late 1990s, including Street Fighter and Marvel vs Capcom. Esports have evolved substantially since then, with several genres providing competitive games, including PUBG, DOTA 2, League of Legends, and Fortnite.

At the very outset, it is important to highlight the differences between esports and gaming, though the two terms are often used interchangeably (**Ayodale, 2019**). Gaming is the playing of video games at a non-professional level, generally as an entertainment mechanism and played for 'fun' rather than competing for prize money professionally. Gaming can therefore be distinguished from esports by understanding that gaming occurs outside

the pool of officially sanctioned competitions involving prize money (**Elchison, 2019**). In fact, what distinguishes esports athletes from casual gamers are the efforts, training, and hours they put in preparing and honing their skills to compete competitively, with studies in South Korea showing that their esports athletes practiced their "sport" for nearly twelve to fourteen hours per day (**Jacobs, 2015**). While this paper discusses the importance of setting a reform agenda for esports, game publishes also have an important role to play in ensuring fairness in gaming generally. As such, throughout this paper the authors have drawn from case studies in gaming and technology used by publishers to prevent cheating in gaming as well as esports.

There has been a long debate about whether esports can be classified as a sport (**Hallmann& Giel, 2018; Brickell, 2017**). The opinion that esports should be considered as a game merely for entertainment purposes, but not professional sports, has been mainstream for quite some time. This was primarily due to a layman understanding of sports which generally relates to traditional athletic formats present in sports such as soccer, cricket, athletics and basketball. Due to its distinct features, which might not fall within the definition of "traditional sports", esports are often labelled as a "non-sport" activity (**Hollist, 2015**). Several organisations acknowledge and provide backup to esports. BundesverbandInteraktiveUnterhaltungssoftware (BIU), a German-based association of producers and publishers of interactive entertainment software, noted that, *"[i]t is not only the motor activity, but it is also the social, cognitive activity that is involved in eSports*" (**Mauch, 2017**). Further, it stated that *"[t]he motor activity is comparable with that of motorsports or chess, in which the motor activity is often not visible... eSport[s] athletes achieve something truly remarkable; with hundreds of clicks per minute, they achieve things that are entirely comparable to athletes in other sports"*(**Mauch, 2017**).A study conducted by German Sports University, Cologne, argues that an esports athlete's physical training and pressure is like that of a traditional sports athlete (**Yun, 2019**). The study states that esports athletes clock a pulse rate of 160-180 beats per minute while they are in a competition, which is equivalent to a marathon runner's pulse rate (**Yun, 2019**).

Increased public engagement and pressure from different organisations led esports to be widely considered a sport (**Kane & Spradley, 2017**). This became significant as it has catalysed the establishment of different governing bodies and specific standards to ensure fair competition. China became the first country to create a governing body, followed by South Korea, the USA and others (**Falcao et al., 2020**). This popularity and recognition led to, in 2017, the 6th International Olympic Committee (IOC) summit, recognising esports as a sport (**Falcao et al., 2020**).

As esports became more organised and gained popularity, the importance of ensuring that fair play and integrity were adhered to became increasingly important (**Holden et al., 2017**). Unfortunately, some players have taken advantage of the lack of harmonised standards and used unethical means to win games. While doping in traditional sporting competitions typically consistent of athletes using performance-enhancing drugs (PEDs) to gain an unfair advantage, doping in esports is slightly different. While the use of PEDs is possible in esports competitions, the types of cheating to gain an unfair advantage in esports are different to that of traditional sports. In esports, in-game cheating is referred to as "e-doping"; which specifically refers to using non-permitted technology in esports competitions (**Holden et al., 2017**). These technologies may come in several forms. For example, players can use specific software or what is popularly known as 'cheat codes' to gain an advantage unethically, or they may even launch a denial-of-service attack (DoS attacks) to disrupt oppositions' gameplay. This is a severe concern for esports, and many steps are being taken to minimise this form of doping in this field (**Brickell, 2017**).

While traditional doping in esports would be the intake of psychostimulant substances like Adderall (commonly used for attention deficit hyperactivity disorder (ADHD) treatment) (**Weyandt et al., 2018**) and other drugs favoured by players such as Modafinil, Donepezil and Propranolol (**Ruef, 2018**), e-doping is different insomuch as it means the modification of hardware and software to give the player a competitive edge (**Abdulaal, 2020**). While intake of substances such as Adderall helps a player remain calmer and increase aggression, e-doping may help a player have the chance to imposeslightly more damage, speed, and accuracy (**Turton, 2017**).

2. MEANS OF CHEATING

As explained above, esports is a multi-billion-dollar industry that engages a significant population throughout the world (especially the younger generation)(**Barclays, 2020**). One unfortunate activity, just like traditional sports that creates an unlevel playing field and threatens to undermine the legitimacy of esports competition, is cheating. Different activities can be performed based on the game, which can come within the ambit of cheating. One such act is the use of performance-enhancing drugs to achieve the desired results. "Desired results" are imperative as athletes are rewarded handsomely for their achievements, resulting in prize money, popularity, and endorsements. Performance enhancing drugs may be used by an esports athlete to achieve "laser-like focus, faster reaction time and alertness, and the ability to predict what other players would do" (**Loria, 2016**). The infamous Adderall case at the ESL One Katowice tournament is one such example (**Loria,2016**). This led to the immediate intervention of the World Anti-Doping Agency (WADA) to compile a list of prohibited drugs in esports(**McCambridge, 2017**).

For leagues and tournament organisers, the use of performance enhancing drugs introduces a complex situation. Shortly after Friesen publicly acknowledged the use of Adderall in the Electronic Sports League (ESL) tournament by his Counter-Strike team (**Scholz, 2019**), the ESL employed the Esports Integrity Coalition (ESIC) to perform drugs tests (**Stiver, 2016**). The Anti-Doping Code of ESIC applies to all ESL tournaments as of February 2016. The ESIC list of banned drugs is included in the World Anti-Doping Code. The list is mainly composed of stimulantssuch as Adderall and the other drugs discussed above.

Perhaps more of a threat to esports than prohibited substances, another form of cheating in esports is using bugs, third party programs and modified gaming peripherals (**Star &Bakshi, 2019**). However, these methods are sometimes considered difficult to prevent by some game developers and security personnel. The following section highlights several key methods that games may use to gain an unfair advantage.

3. BOTS & TECHNOLOGY ASSISTANCE

Aimbots and triggerbots: An aimbot is a computer bot used in multiplayer shooting games most commonly to offer numerous automated targets and calibration for the player(**Star &Bakshi, 2019; Michaeli, 2020**). Triggerbots may be used with an aimbot to automatically shoot when the opponent player approaches within the shooting region aiming towards the reticule of the opponent like an instant reflex action. An aimbot receives the details of the entire player relying on each player's in-game character's positioning and checks whether the opponents are visible or not from their position. Targeting (commonly prevalent in point and shoot games) is the process of a player determining the location of their opponent and pointing their weapon towards them. This targeting works like a professional gamer when done through an aimbot as the targeting is now automated. Cheat suites comprise similar features in addition to this, including ammo count, move speed and player radar (**Hao & Tan, 2021**).

Artificial lag/tapping: Here, peer-to-peer access is utilised to access the game. Lagging is done among one or more players when the data streams are manipulated, slowing down the game or interrupting during the game pausing character movements or distorting the opponent's play. Lag switch stops the upload of commands from the player to the game server. The aim is to win over the opponent without reciprocation. The opponent character stops or slows down, allowing the lag switch to control the game entirely. From the opponent's view, the player can either teleport, be invincible or invisible while he suffers delay in the graphics within seconds **(Cole & Hooley, 2013)**. The gaming community refers to this process as "tapping" as it takes one tap to connect and disconnect the internet connection and perform the lag **(Rietkerk, 2020)**.

The lag switch comprises different methods that disrupt the network's communication between the server and the client. The most popular method of lag switching is by connecting a physical device known as a hardware lag switch with the ethernet cable. Switching on and off disrupts the connection. Video game console hardware has been designed to protect against such intentions by introducing the built-in solution like voltage detectors against the lag switch. The voltage detectors can detect whenever there is a slight change in the voltage. However, some gamers have taken specific measures such as unplugging the ethernet cable connected to the client-server, causing the desired disruption in the player's internet connection. Other hacks such as software lag

switch or wireless lag switch requires a computer program to run on the system of the cheater connected to the same network as the players. Disruption caused by the application then results in disruption of the communication between the server and client (**Mitchell, 2020**). However, this cannot be done for an extended period as there will arise a situation where no traffic will be received, which will make the client game server think that the connection has been lost and will remove a player from the game. Some more advanced level methods include firewall or router rules which apply bandwidth by structuring the network latency. An athlete thus adjusts the limits on that bandwidth and latency to keep them connected to the peer-to-peer network while having constant advantages over the targeted players.

Look-ahead: This also requires a peer-to-peer connection to cheat in a multiplayer game where the client cheating gains a benefit by causing a delay in their actions. By using this method, the client acts as the victim of high latency: the outgoing packet is made as to the actual packet by attaching a timestamp with it, thus fooling the other clients by making them believe that the action was done at the correct time, but itdelayed in the arrival. A probable solution to this cheating is the vanilla lockstep protocol **(Huynh &Valarino, 2019)**.

World-hacking: World hacking is a third-party program that exploits bugs and displays more levels to the player than the actual game levels. Visibility depends on the Fog of War **(Kanaan, 2020)**. Fog of War is the mechanism to enable the display of gaming objects by limiting the player's access. This mechanism is used by the world hacking concept used by the player to bypass the in-game mechanics either by creating a fog to render objects or by removing the player entirely. In multiplayer settings, the user is more advantageous than other players in average real-time strategy games. It may also offer a player the chance to see through objects to know before the arrival of an opponent. This includes the process of transparent wall textures or modifying maps of the game to insert polygonal holes in the wall. This process is known as a "wall-hack" as it allows opponents to see through walls **(Sparrow et al., 2020)**. World hacking depends on the fact that the FPS server will send the other players' positions, and thus hiding the opponents behind the wall depends on the client's 3D renderer. Hiding the whole map does not offer an advantage to the cheater as it cannot navigate the pathways and obstacles. However, if ever an outline is visible, the hacked user will be able to navigate. Recently, the wireframe display driver released by Asus enables players to utilise wallhacks, which is set as "special weapons" that user could use in multiplayer games. Graphics are used to show wireframe drawings **(Marquardt et al., 2019)**.

Removal of the game element: Removing the elements will offer the user to get rid of the game's annoyances or inhibitors. These include bullet spread or elimination of weapons **(Hollis, 2018)**. Removals result in a decrease in the skill requirement of the user. *PokemonGo*was the victim of this malpractice **(Paay et al., 2018)**.

Exploiting: Exploiting is an application wherein an unintended feature or bug offers players a benefit **(Rhodes,2019)**. Most gaming software restricts this practice and sanctions against the player if caught cheating. It can be argued that exploiting is not completely cheating as it uses advantages already provided in the application. This is also considered a skill by some as it needs concentrated efforts to understand the lacunae in the game to exploit.

Character sharing: This method is a commonly used form of cheating. Sharing with people as a single character, primarily in Massively Multiplayer Online Role-Playing Game (MMORPGS), gains advantages by spending much time each day by levelling and comprising higher stats than usual. This can be differentiated from normal 'levelling-up' in games because this artificially makes a Level-10 (for example) character compete against a Level-1 character, thereby creating an unfair competition. Thus, MMORPGS is a reverse engineering method **(Tomicic et al., 2019)**.

Secret alliances: This practice is also known as "teaming", as this form occurs when multiple players engage themselves in maintaining a secret, unofficial advantage of the game to help them win against the other players. Teaming helps in balancing difficulty levels and providing suggestions **(Haahr, 2017)**. This can be done in games that have free for all deathmatch or last man standing mode. The nature of this kind of cheating is when players engage themselves in secondary conversations with each other using another software to navigate screens of secret allies while one of them playing offers tactics or advantages over other players. This type of cheating is complex in some kinds of games because it is difficult to prove that cheating has been done. The admins of the gaming server, who are monitoring the whole game, cannot catch players engaging in this kind of act.

Stacking: This involves changing game settings or teaming up to offer one or more players an unfair advantage. One such example is an arrangement of a team with high skills against a team with low skills. Although this could be considered an essential practice in real-life sports, gaming becomes an issue for less-skilled players. Stacking share and actual share together reveal the cheating image, much like the stacking prevalent in Enron where employees were stacked according to their performance, leading to unfair advantages of one team over the others**(Blackburn et al., 2013)**. Rigging involves weighting the game in favour of one player or team by offering a particular set of circumstances to the player or team with better or familiar weapons or establishing a battlefield that caters to their strengths. This also results in the creation of unequal teams such as "five vs ten" matches. Some games prevent this practice by not allowing more players options when uneven teams are created, offering a certain balance.

Scripting: Scripting is a practice that includes a software or program to automate some action in the game. Some might consider this not to be cheating, depending on the behaviour of the characters, and depending on whether that behaviour is replicable without the use of script cannot be said. For example, a predictable script provides the user increment in firing speed or may perform trivial tasks such as reloading the gun. Unfortunately, scripts also acquire the power to tamper with other player's systems by spoofing commands by writing codes **(Rollinger, 2020)**.

Collusion: In esports, one means of cheating is colluding with other players to gain an unfair advantage using their support. For example, "win trading" can be considered a form of colluding, which has widely happened in the game of StarCraft (**Torres, 2007**). Two players collided with each other, and each of them lose against the other alternatively in the ladder competition. The loss taken by the opponent would provide a victory point to the other by raising its ladder rank. Therefore, both players can now top the game winners list by not even playing a fair game since this would increase their number of wins and therefore points on the points ladder.

Abusing the game procedure: Players can use this method without any technical sophistication as they do not need any technical skills, rather it only requires them to deviate from the gaming method. A typical case observed which resembles this scenario is "escaping" the game. Players may, for example, disconnect themselves abruptly from the game if they are losing. Another way is scoring cheating, which was observed in the popular game Go, adapted from a traditional Chinese boardgame. According to the rules of the game, after finishing, the player must remove the "dead" stones by hand before judging who won the game (**Iwamoto, 1977**). However, to cheat the system, the player, during the scoring process, removes the "alive" stones of their opponent, thus transforming the game's result.

4. IMPLEMENTATION OF CHEATING:

While the previous section set out the different forms of cheating, this section will explain how these formsof cheating are implemented. Among the client-server model, the server is the security provider which enforces

gaming rules. Despite running equal code in the peer-to-peer gaming model, clients still face the same type of cheating found in multiplayer models.

"Clients can never be trusted" is a saying among the gaming admins that sums up the gaming design of the client-server model **(Reis Cecin et al., 2004)**. It means no client could listen even once if they break the game's rules or primary mechanism, and no information must be sent to the client unless it is a "need to know" option.

Game code modification: In many cases, cheating is done by modifying the software according to the user's benefit, except EULAs (End User License Agreements) restrict modification of the code **(Consalvo, 2009)** which may lead to adverse consequences for the player, including being banned from the game. Gaming software prepared in binary-only versions also forbid modifications, making only reverse engineering possible. Game data files can also be changed from the main program, thereby circumventing the protection built in the software by the developers.

System software modification: Instead of editing the gaming code, some players modify the underlying system components. An example of this is the modification of the graphics driver that ignores checking in detail and draws objects on the screen like wall hacking **(Fuentes &Mercês, 2019)**. This practice is the toughest to detect due to the presence of variation in many systems.

Packet interception and manipulation: The gaming model's security can be intervened by intercepting and manipulating data in real-time during the transition of the server from the client or the opposite. Manipulation or interception can be of passive or active form; any methods can be performed on the user's machine or through an external communication proxy. Some aimbots use this method too. Network traffic must be obfuscated to avoid such attacks **(Lozano, 2017)**.

5. E-DOPING PREVENTION PROTOCOLS:

The use of performance enhancing drugs in sport is a severe threat to the spirit of sports **(Newton, 2018; Kambhampati& Star, 2021)** and the same is extended to esports. Reports of doping incidents in different tournaments have raised questions about the credibility of such competitions. Thus, the institutions in charge had to implement regulations to ensure that such incidents are kept at a minimum **(Hilvoorde& Pot, 2016)**.

Electronic Sports League (ESL) is the leading organisation when it comes to regulating prohibited substances in esports. The ESL promotes the regular conducting of tests of participants. This can be a challenging task, but the ESL is currently working in compliance with agencies that conduct drug tests for traditional sports. The tournament participants must go through a simple saliva test **(Nunes&Macedo, 2013)**. If they test positive for prohibited substances, they cannot participate in the competition (or their results are annulled) and further disciplinary action may be taken. Several gaming companies also conduct tournaments and test their players. For example, EA Sports conducted mandatory drug tests for all the contenders taking part in the FIFA esports world cup tournament **(Martinelli, 2018)**. However, the prevention of the used of prohibited substances in esports competitions is a challenging task for organisers, especially when the players are not physically present in an arena.

The challenges of preventing doping in esportsbecome more complex when factoring inthe various forms of e-doping. To this end, players can often avoid detection when using illegal software (or hardware) as it may not be possible to check everyone's system, particularly for remote and online users. Thus, it became evident that technology can only be countered with technology. Hence, the relevant governing bodies and game publishers have implemented specific ways of preventing such technological exploits by using anti-cheating technology themselves (**Denuvo, 2021**). Some of these prevention tools and strategies are discussed below:

Valve Anti Cheat: Valve anti-cheat (VAC) is a software that Valve has developed to prevent players from using non-permitted software hacks **(Witkowski, 2012)**. The software used by the company is not publicly disclosed, as it would then help the cheaters find vulnerabilities in the system. However, it is known that VAC, through deep learning methods (**Kedziora et al., 2020**), uses signature scanning and accesses the system's memory and processor and tries to find if the user is using any cheat. If the system detects any anomaly, that piece of code is copied and compared with an existing database of discovered hacks. If the code matches another one in the database, it is confirmed that the player was cheating. If the code does not match, it may be inspected

by the Valve engineers, and they might try to analyse it or run it on their system. If they are convinced that the code helps in cheating, the proper action is taken, and the code is added to the cheats database. To ensure the security of the system itself, the system is updated regularly and is sent in small portions to the servers. Valve also encourages submissions from players on new cheat software and websites. Players can also report other players if they are suspicious of their activities. If a player is found cheating, actions are taken against the player by the company (**Lehtonen, 2020**). Usually, this means that the player is banned from that specific game. Other games that are in partnership with Valve (such as Counter-Strike, Day of Defeat and Team Fortress) may ban them as well. The best thing about VAC might just be the fact that it can be effectively integrated with other anti-cheating mechanisms too (**Webb & Soh**, **2007**), thus making it truly versatile.

Design of the Server: The server design plays an integral part in ensuring that the players cannot cheat **(Lehtonen, 2020)**. This server design is often referred to as authoritative and mirrored server design. Two different approaches can ensure the better design of servers. One approach makes the client functionality run on the server of the game itself. This is the authoritative model. The mirrored service design mirrors the gameplay of the client. If the player is cheating, the session is out of sync. This prevents cheating. However, this process can cause the system to lag. This was a considerable concern some years ago, as the computational capacity (like processing speed) of the player's system was not very good. Many users often had a slow internet connection as well. These factors, combined with the increased hardware and implementation cost forced the authorities to compromise system security to ensure smooth gameplay. However, today these costs are much lower, and a fast internet connection is much more readily available. Hence, these have become much less of an issue today **(Duh & Hua Chen, 2009)**.

Software Obfuscation: This refers to the runtime protection implemented by specific games. Gaming developers use software protectors to serve this purpose. The aim is to ensure that the attackers cannot directly inspect or modify the software **(Xu & Liu, 2016)**. This can be done in three ways: encryption solution, runtime decryption and virtualisation. The first type encrypts the code and uses a multi-layered model to prevent the player from reversing or tampering with the code. Here the encrypted code is decrypted only when the game is starting or running. The second approach is runtime decryption. Runtime decryption may cause some problems, for example, the game may experience lowered frame rate, and the process may be slowed down. The third alternative is the strongest one: virtualisation. In this process, the encrypted code is run on a different CPU with unique configurations compared to the generic CPUs **(Liu & Jia, 2015)**.

Supervision of Players: Player supervision is when the administrators of a game server monitor individual players and check whether any hacking is taking place. However, there is a risk associated with this approach. Certain players may feel like this allows the administrators to spy on specific players and tell opposition players their secrets (including tactics and positioning). This would lead to significant challenges in competitive matches. Some games counter this problem by delaying the video feed for the supervisors, while some games do not allow any spectator mode **(Bursztein et al., 2011)**. In some other games, there are provisions for supervising players by the community itself. This can be done by providing screenshots, videos and similar information to the admins. The users can report specific incidents like disruptive behaviour. The administrators will then review whether these reports are accurate and to what extent.

Statistical Approach: This approach uses statistical methods to determine whether there is an anomaly in player behaviour in different game stages. This is done by statistically analysing the player's activities. The most significant advantage of this approach is that it does not invade the privacy of the players, and it also works on all systems. However, there is a significant drawback of this system as well. This system cannot objectively identify whether a player has cheated or not. Very highly skilled players are sometimes considered cheaters, as their skill level is very high, and the computerised system may not understand that. Also, certain players may find ways of beating the system by cheating in a way that the system cannot detect. To overcome false positives, this system is often used alongside other supervision systems managed by professionals. In this process, the unusual behaviours of the suspected players are recorded and sent to the respective administrators **(Lehtonen, 2020)**.

Pattern Detection: This approach works by scanning the hard drive of the players' systems. This is done to check whether there are any known cheat codes. Here even the subtle incidents of cheating are detected, which

are overlooked by statistical methods. However, the system needs to be kept updated. There are also privacy concerns for the players with this approach **(Thomas &Kadish, 2021)**.

Sandboxing: Sandboxing is a process that is used to prevent cheating while playing. It prevents malicious functions from running **(Borate & Chavan, 2016)**, for example, code injection and memory modification. Since the cheat mechanisms do not work, there is no need for banning players from the community. This can be a significant advantage of this system. This does not cause an invasion of privacy either.

6. SANCTIONING PROTOCOLS

There are several ways of preventing cheating across significant tournaments. However, these are not always useful as players may find new ways around these protocols and indulge in e-doping. Then it becomes necessary to take appropriate steps to sanction players who violate the rules. However, it must be remembered here that no central regulatory body in esports exists that determines the sanctions for such acts. Rather, sanctions are handed down by the administrators of a particular game, or a tournament organiser. Hence, there is a lack of harmonisation when it comes to sanctioning protocols for e-doping. Consequently, different games and different tournaments implement their own standards. Players are often banned from games or leagues if they are found to be doping or cheating. Sometimes the whole team is banned if one team member is cheating, such as Polish team TajemniceWatykanu (Secrets of the Vatican), who were disqualified from the Polish ESL Championships eliminations (**Jasny, 2020**). This is consistent in traditional sports too, where if one team member in a relay team is found to have doped, the results of the entire team will be disqualified. This can have a considerable economic impact on professional players, as they may be required to move to lower leagues or banned from the game. Sponsorship contracts may also be cancelled if such incidents happen as sponsors may no longer wish to be association with that player or team (**Freitas et al., 2021**).

In some cases, players may be fined as well. In some scenarios, the offender may have to appear before a disciplinary panel or court if cheating is considered a crime in a particular jurisdiction **(Heubl,2020)**. The usual steps that gaming companies take towards cheaters are described below:

Imposing a ban on players: Certain companies and leagues take this step to punish cheaters. If someone is suspected of cheating, the company usually reviews his activities on the game. If the allegations against the player are proved to be accurate, the company or the league has the power to blacklist them, as in the case of Newbeebeing banned from professional Dota 2 in China **(Stubbs, 2020)**. Importantly, the user is bound by certain rules under the end-user agreement and the consequences of these rules may result in a ban or suspension (**Adinolf&Turkay, 2018**). This is done by preventing the installation of specific programs or serial keys. Sometimes the online account of the player is also banned. This means that the player cannot play the game online anymore. There might be extreme cases where a person has done considerable damage to the game, such as ruining the experience for others or some other activity that has ultimately led to user dissatisfaction and loss of revenue for the company. It is not uncommon for the games to completely ban players from playing the game in such cases. This must be done from a hardware perspective and hardware ID or IP addresses are commonly used. In most cases, the publishers are reluctant to reveal the exact number of accounts that have been banned. Companies such as CipSoft have banned players in batches previously and such bans have been revealed by the companies afterwards **(de Paoli & Kerr, 2009)**. This is an effort to deter other players from cheating. However, it must be remembered here that a ban is not always applicable. In case of hardware bans, the player can use a Virtual Proxy Network (VPN) to continue playing the game. They may also change their hardware configuration to render the ban useless.

Shadowbanning: Shadow banning does not involve stopping anyone from playing the game. However, if one user is found to be cheating, the game administrators match-up users such that they can only play with other players who have cheated. This prevents the cheaters from knowing that they have been identified by the administrators. This can be a practical approach because if the player is not aware that they have been spotted, they will not take steps to circumvent the situation, which is a genuine possibility in the case of the usual banning. **(Parungo, 2021)**.

Suspension: A suspension is a temporary ban which expires after a certain period. This approach is taken when the cheating methods employed by the player are not too serious. This may involve abusing glitches of the

game, benefitting from malicious hackers or harassing others, depending on the severity of the situation. It is common when a cheating activity is detected by supervision or statistical approach. Sometimes game publishers take resort to suspensions if the violation cannot be proven without a doubt **(Singh, 2021).**

In-game kicks: Compared to the above two sanctions, in-game kicks are a relatively minor consequence from a player's perspective. It is generally used if the game publisher wants to issue a warning rather than hand down a strict punishment. This is also used when the integrity of the system cannot be proven without suspicion. It is more of an instant punishment for relatively minor infraction. This is usually handed out to players with questionable gameplay behaviours. Many publishers also let the game's community determine the player who should be banned, sometimes through a voting system. Under such an approach, actual players carry out the entire activity, and decisions are taken based on votes. So, if many people report suspicious activities by a player, there is a high chance of them having cheated. It also removes the need for supervision and other anti-cheat methods. However, one significant disadvantage of this mechanism is that legitimate players also stand the risk of being kicked out of a server. This happens when false reports are generated by other players, usually as a means of making fun of someone or out of personal grudges. Hence game publishers need to be careful while employing this technique. Another concern that may be encountered by innocent players is when they are kicked out of a game due to mere inactivity **(den Bosch, 2021)**.

Demotion: In some instances, a ban or suspension may be too harsh of a punishment. In such cases, the publishers may decide to let the player continue playing the game, but their ranks are lowered, meaning they are moved to a lower rank of players **(Stavropoulos, 2020).** This is usually the standard protocol if the offender is caught farming or stat-padding.

Progress removal: Progress removal can be considered as a harsher version of demotion. Instead of demoting the player to a lower rank, in this case, their real progress is removed, and the player's score is reset to the base value that is assigned to someone who has just opened an account in the game **(McNeil, 2020).**

7. LEGAL FRAMEWORK

There is a lack of standardised regulations in place to determine sanctions for e-doping. This is often because unlike traditional sports, no central regulatory body will determine these laws **(Chao, 2017)**. In addition, cheating in esports is a complex issue given that there can be different means of gaining an unfair advantage. In single-player games, various cheats are often used and have been ongoing for a long time. However, this is not usually considered a punishable offence. This is because there is no other person involved in this process whose gaming experience is being hampered.

Another form of cheating is when players cheat within a multiplayer contest. They can use several different methods, often referred to as hacks, to get a competitive advantage over their opponents. This is a more severe issue, and it hampers the gaming experience of others **(Abarbanel& Johnson, 2020)**. Another critical point to be considered here is the age of microtransactions in online games **(Derrington et al., 2021)**. There are often different services or features that are unlocked only after the player purchases them. They are primarily available in the form of "packs", which involve in-game transactions **(Macey et al., 2020)**. These services are often meant to provide certain advantages, which are only exclusive to purchasing them. However, gamers may find ways to gain access to these services without purchasing them through illegal sites. In that case, it can be considered a direct loss of revenue on the company's part. Despite this being the case, there is a lack of enforcement in many cases to stop such incidents from being happening strictly. One reason for this may be the adoption of large-scale anti-cheating methods and enforcing them on everyone may prove to be more costly than allowing specific hackers to cheat.

In many cases, the accounts of the offending players are banned either permanently or for a certain period. However, it is relatively easy for the culprit to open another account, as these games typically do not usually need a unique identity to create an account. However, it is to be remembered that creating game mods (modifications) that allow users to cheat has much more severe implications unless the person has been authorised to do so by the company. Video game creators are protected by the terms of services that a user must sign before the game can be played. Recently a law has been passed (by amending the Game Industry Promotion

Act) in South Korea that states any person found guilty of committing such a crime will have to face a fine of US$ 34,000 or imprisonment up to five years **(Good, 2018)**.

A more serious offence is when a player cheats in a professional tournament involving prize money. In these cases, punishments are much more strictly imposed. This may involve a ban from the game or tournament, monetary fines or even court cases. In addition, there have been instances where the company has sued players for e-doping. Some case studies of hackers getting caught by the organisers of a tournament or a game have been mentioned here for this purpose:

CASE 1: AZUBU FROST vs TSM

In Season 2 of the League of Legends World Championships in 2012, the Azubu Frost Esports team members were caught looking at the audience's screens to know the location of TSM members on the map **(AviarysNation, 2012)**. This resulted in a US$ 30,000 fine that was imposed on Azubu Frost for cheating.

CASE 2: NICK EH 30

Nicholas Amyoony, better known by Nick Eh 30, is a Canadian YouTuber and a Fortnite Pro player. He was caught cheating in a charity esports game, where he refused to land in the specific locations mentioned in the tournament rules **(Fortnight Kid, 2020)**. The rule was in place to ensure healthy competition, but it also stated that offenders would be let go with only a warning in time. Nick Eh 30 was aware of this rule and refused to follow it. So, as a consequence of violating this rule, he received a warning.

CASE 3: SHAIIKO

French professional Rainbow Six Seige player, Shaiiko, was involved in a match against Penta where Shaiiko was accused of cheating. An investigation was carried out, and it found Shaiiko guilty of constantly pressing the number '4' key that gave him an unfair edge, which was against the rules of the game. As a result, Shaiiko was banned for two years **(TheScore esports, 2020)**. He returned to the professional gaming scene in 2019 and performed well. Shaiiko has been involved in gaming actively since then, and it appears that he has moved on from this cheating scandal and the subsequent ban.

CASE 4: FAZE JARVIS

FaZe Jarvis was an esports player whom Epic Games already banned from playing Fortnight for previous misdemeanours **(Hernandez, 2019)**. However, he later created another account and continued to play. While actively involved in gaming in a live stream, he wanted to check whether Fortnite's anti-cheat technology was working and how efficient it was. The incident ended with him being banned again **(Dey, 2021)**. However, this case study points out the ease at which banned players can create new accounts and return to playing again.

CASE 5: KQLY

KQLY (HovikTovmassian) was a very popular Counter-Strike: Global Offensive (CS: GO) player from France. He had won multiple tournaments, including the Electronic Sports World Cup in 2013. He was held in very high regard among the CS: GO community. In 2014, he was involved in some sort of cheating detected by VAC **(HLTV.org, 2021)**. As a result, KQLY received a VAC ban, but the exact reason was not disclosed.

CASE 6: JONATHAN KOSMALA

Fortnite player Johnathan Kosmala, more popularly known for his gaming tag "JonnyK", was got caught while using a hack **(Chen, 2019)**. This activity came to light after the cheat creator partnered up with YouTuber 'The Fortnite Guy' to disclose the incident. His type of hack was a wallhack that enabled him to spot players who are behind walls or other obstacles. After the incident became public, Kosmala was released from his team, "Team Kaliber" and Kosmala's reputation suffered a big blow after this incident because the tournament he was cheating in involved significant prize money of US$ 30 million **(Valentine, 2018)**.

8. CHALLENGES FOR IMPLEMENTATION OF ANTI-DOPING PROTOCOLS

There are several challenges in implementing anti-doping protocols in esports. Traditional sports have regular drug tests to check whether any prohibited substances are present in their bodies. However, comes at a significant expense **(Henneberg, 2014)**. It is estimated that the cost of implementing such measures can amount

to as much as US$ 40,400. This makes such testing possible for only big leagues such as the ESL, which have conducted anti-doping tests since 2016. However, the lower leagues suffer budgetary constraints. These lower leagues often act as the steppingstones before players break into the big stages. In addition, there are now sizeable betting markets on such tournaments. Accordingly, it is important to ensure fair play in these competitions. Another significant factor in this scenario is that there is no central governing body responsible for allocating funding for such testing unlike traditional sport where international federations and national anti-doping organisations coordinating the testing of athletes across sports. Hence, there are no standard procedures or benchmarks with respect to implementation of anti-doping protocols across esports **(Martinelli, 2018)**. Different games and different leagues implement their own standards. Traditional sports have been dealing with these issues for many years. Much money is spent every year on dope testing of athletes, but significant problems still exist today with respect to detection of performance enhancing drugs in sport. Compared to these sports, esports tournaments have much smaller budgets and experience in handling such cases. Hence the abuse of performance enhancing drugs becomes much more difficult to police.

Traditionally, dope testing requires all players participating in a particular tournament to be present physically. While this is typically the case for large esports tournaments, there are many competitions where players participate remotely, and under such circumstances it is more difficult to conduct these tests. Moreover, there are differences in the legal opinion on whether intake of substances like Adderall should be allowed (**Chung, 2019**). In additionto these physical forms of doping, these remotely participating players can use several software hacks to gain an advantage over others. While an increasing number of methods are being developed to stop this, some players will inevitably look for opportunities to find new ways of beating the system, which can make regulating of e-doping a challenge (**Bafna, 2020**).

The actions taken by the gaming companies are also sometimes not entirely effective. Some games ban an account if there are reports of cheating. However, the player can always use another account to log in to the game. Given the fragmented nature of governance in esports, there are instances when a player has been banned from a particular league for e-doping, and the player has subsequently moved on to another league where their sanction is not recognised. Given the resource constraints of some minor leagues, the organisers often cannot check each player's background and, consequently, they may let everyone compete. Hence, this problem is complex and has no clear path that can be followed **(Hollist, 2015)**. Nonetheless, given the exponential rise of gaming and esports and the growing concern of e-doping, reform is warranted to mitigate these concerns and promote fair competition.

Implementation Challenges

Former WADA head, David Howman, has pinpointed the lack of anti-doping policy in esports and governance issues **(Baldwin, 2019)**. As the central regulatory body, adherence to a homogeneous anti-doping regulation seems a far-fetched dream, especially in the context of a fragmented esports ecosystem that seem divided on the point of allowing or wholly banning prescription drugs **(Hamstead, 2020)**. The mission of player protection, integrity and fraud prevention will be difficult if a direction is not given to the esports industry **(Kelly et al. 2021)**. Due to the lack of a proper governance system, an athlete banned by one league based on malpractice can quickly shift to another league without any significant surveillance. Thus, it is important to create an international regulatory body that oversee the governance of esports. Domestic governing bodies around the globe can replicate the governing model made by this international body for a clean esports environment.

Another issue is that of legal recourse. Article 8 of the International Esports Federation (IESF) Anti-Doping Rules states that any dispute arising out of anti-doping violation shall be heard before the "Hearing Panel" of the IESF. The same can then be referred to the Court of Arbitration for Sport (CAS) under Article 8.4of the Rules (**Chanda &Vuyyuru, 2021**). Unfortunately, the CAS, since its inception, has decided on traditional doping matters and is perhaps not yet experienced e-doping scenarios (**Martinelli, 2018**). It shall be interesting to see how the CAS will respond to e-doping matters when they arise. Nonetheless, it arguable that internal disciplinary tribunals (of each game) are best placed to deal with these disputes, at least at first instance.

9. RECOMMENDATIONS

While there are lessons to be learned from best practices in traditional sports when considering reform in esports, one has to be careful not to paint the picture with the same brush. They come from different contexts and reforms must be design with these different contexts in mind.

- **Governance reform:** Some scholars have argued that esports would benefit from an international regulatory body and, through that regulatory body, a set of homogeneous rules and regulations **(Georgiades, 2021)**. However, it needs to be acknowledged that given the fragmented nature of the esports ecosystem, and the control that publishers and game administrators have over various games, that creating an overarching governing body may be difficult in practice. Consequently, other scholars have argued that promoting a governance framework that promotes best practice governance principles would be a useful starting point **(Kelly et al., 2021)**. Governance reform would promote consistency across esports. This would enable international leagues and tournaments to standardise their anti-doping and integrity regulatory framework, which would be extremely helpful for promoting fairness for the competing athletes. It should also be noted that inter-league integrity and transparency is imperative. Therefore, various leagues that organise tournaments should share sanctions imposed on athletes due to e-doping, and other leagues shall exercise participation bans of such an athlete. In practice, this can be achieved even without a single regulatory body, through agreements between leading tournament organisers, or under the guidance of institutions such as IESF or ESIC.
- **Developing a clear policy and research agenda:** Putting doping in esports and doping in traditional sports in the same bracket might seem unfair to certain scholars, but then some scholars also argue for similar treatment in both**(Cheng, 2019)**. Both these formats are exclusive and thus need an exclusive anti-doping regulatory framework that extends to both performance enhancing substances and other forms of e-doping. Therefore, federations should act with caution while deciding on the prohibited list for esports and shall only ban substances and procedures that will genuinely give an advantage to an esports athlete. While policymakers and regulators in esports can learn from the experiences in traditional sports, it is imperative that the unique context of esports be considered**(Kelly et al., 2021)**.
- **Dispute resolution in esports:** With the flourishing esports scenario, e-doping matters may become more regular at the CAS (through an expansion of the scope of Article 8 of the IESF), and for that, proper redressing structures are required. The traditional structure for dispute resolution which is available for each sport could be modified according to the needs of esports, but the basics of dispute resolution remain the same (**Blum, 2016**). Perhaps for e-doping matters, members and arbitrators who understand e-doping must be appointed on the CAS arbitrator list, and proper dispute resolution guidelines, including with respect to evidentiary burdens and procedure, must be prepared for redressing e-doping matters.
- **Contractual amendments:** As is often the case in traditional sports, employment contracts and professional athlete agreements often contain a “morality clause” that aims to regulates the behaviour of the athlete. The clause enables federations, clubs or employers to terminate an athlete’s contract if they are caught doping or engaging in any conduct that undermines the legitimacy of the sport **(Holden et al., 2017)**. It is in both the commercial interest of stakeholders, and also the interest of esports generally, that esports players are deterred from engaging in e-doping. Including such clauses may go some way in achieving this.

10. CONCLUSION

With the rise in popularity of esports, its dark sides have also become apparent. E-doping is one such phenomenon. While the use of performance enhancing substances takes place in traditional sports and esports, it is perhaps more difficult to police the use of such substances in esports for several reasons. First, most tournaments do not have specified standards and regulations. Even if they do, it is challenging to implement these due to low budgets compared to traditional sports. In addition, unlike traditional sports, in some esports competitions players are not present physically in the arena but operating from different locations, often

worldwide. However, the most significant problem with doping in esports is when players use restricted technology to win games. There are various ways a player can cheat, depending on the game they are playing, including the use of aimbots and lag switches. E-doping is sometimes difficult to detect since the users' systems are not always accessible to the moderators. However, several attempts are being made to counter cheating using technology with technology. VAC is an example of software that can detect certain cheating activities, while other methods used to minimise e-doping are designing special servers and using statistics. However, despite improvements in technology to counter e-doping, the lack of a universal governing body creates several problems in esports. Players banned by one tournament are often shifting to others which may not perform proper background checks, perhaps due to resource constraints.

Though video games have been on the market for several decades, the fact that competitive gaming was adopted as a professional sport more recently is worth noting. The exponential growth of esports has increased the commercial benefit for many stakeholders in the industry and it has created an urgent need to preserve the booming sector's integrity. The operational regulations and identification of hacking are incorporated in the contexts of competitive online gaming to prevent manipulation and promote fair play. However, the infringement of "unwritten" regulations and local implied standards is more difficult to follow.

Some commentators argue that the most practical way to deal with the issue of e-doping is to ensure an international controller regulates and a set of homogenous laws and regulations through a regulatory body. If such a central authority were to be created, it would allow international leagues and competitions to standardise their regulatory anti-doping structure, which would be beneficial for competing athletes. Ultimately, encouraging fair-play and raising awareness about the problems of doping and e-doping amongst stakeholders is in itself an important step. As such, inclusive discussions with all the stakeholders such as players, gaming developers and publishers, esports federations and tournament organisers should be the way forward. With the development of clear governance standards and high standards in competitive gaming, the legitimacy of the esports industry will be strengthened, and the future of esports as an industry will be more sustainable.

11. References (APA)

1. Abarbanel, B.& Johnson, M.R. (2020) Gambling engagement mechanisms in Twitch live streaming, *International Gambling Studies*. 20:3, 393-413. DOI: 10.1080/14459795.2020.1766097
2. Abdulaal, A. M. (2020). Sport Corruption: The Case of doping in eSports (Master's thesis, *HøgskoleniMolde-Vitenskapelighøgskoleilogistikk*), 16.
3. Adinolf, S., &Turkay, S. (2018). Toxic behaviors in Esports games: Player perceptions and coping strategies. In *Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts.* 365-372.
4. AviarysNation, (2012). Proof Azubu Frost Cheated vs TSM!.*AviarysNation, YouTube.* Retrieved: https://youtu.be/yW7uNxqXfn8
5. Ayodale, S., (2019). Esports vs. Gaming: What's the Difference?.*Taylor Strategy*. Retrieved: https://taylorstrategy.com/esports-vs-gaming-whats-difference/
6. Bafna, P. (2020). Challenges to the Anti-Doping Regulations in Esports. *J. for Sports L. Pol'y& Governance*, *2*, 133.
7. Baldwin, A. (2019). Doping: Drug testing methods stuck in the 1970s, says former WADA head. *Reuters London.*Retrieved: https://www.reuters.com/article/us-sport-doping-idUSKCN1RS1DO
8. Barclays. (2020). Gen Z are shooting for careers in the video gaming industry, *Barclays.* Retrieved: https://home.barclays/news/press-releases/2020/01/gen-z-are-shooting-for-careers-in-the-video-gaming-industry/
9. Blackburn, J.,Kourtellis, N.,Skvoretz, J.,Ripeanu, M. and Iamnitchi, A.(2013). Cheating in Online Games: A Social Network Perspective.*ACM V, N, Article A*. 20.DOI: 10.1145/0000000.0000000
10. Blum, B. (2016). Power dynamics in esports: developing alternative dispute resolution. *ESPN*. Retrieved: https://www.espn.in/esports/story/_/id/15600111/developing-alternative-dispute-resolution
11. Borate, I, and Chavan, R.K. (2016). Sandboxing in Linux: From Smartphone to Cloud. *148 International Journal of Computer Applications.* DOI: 810.5120/ijca2016911256.
12. Brickell, A. (2017). Addressing integrity and regulatory risks in esports: The responsibility of the whole esports community. *Gaming Law Review*, *21*(8), 603-609.
13. Bursztein, E., Hamburg, M., Lagarenne, J. &Boneh, D. (2011). Open conflict: Preventing real time map hacks in online games. *In 2011 IEEE Symposium on Security and Privacy*. 506-520.
14. Cambridge Dictionary. (2021). E-sports. *Cambridge Dictionary*. Retrieved: https://dictionary.cambridge.org/dictionary/english/e-sports
15. Chanda, S. &Vuyyuru, T.R. (2021). Time to be grown-ups about e-doping? *Extra-Cover: The Sports Law Blog of India*. Retrieved: http://hdl.handle.net/10739/4726

16. Chao, L.L. (2017). You must construct additional pylons: Building a better framework for esports governance. *Fordham L. Rev.*, *86*, 737.
17. Chen, E. (2019). Team Kaliber Fortnite pro kicked for attempting to cheat in World Cup. Daily Upcomer. Retrieved: https://daily.upcomer.com/team-kaliber-fortnite-pro-kicked-attempting-cheat-world-cup/
18. Chung, E. (2019). Gotta Catch 'Em All! The Rise of eSports and the Evolution of its Regulations, 22 SMU SCI. & TECH. L. REV. 231. 239-242.
19. Consalvo, M. (2009). Cheating: Gaining advantage in videogames. *MIT Press. ISBN: 9780262033657*. 1-240.
20. Cole, S.H., & Hooley, J.M. (2013). Clinical and personality correlates of MMO gaming Anxiety and absorption in problematic Internet use. *Social Science Computer Review*. 31(4), 424-436. DOI: http://dx.doi.org/10.1177/0894439312475280
21. De Paoli, S. & Kerr, A. (2009). The Economy of Cheating InMmorpgs: A Case Study Of Innovation. *MCIS 2009 Proceedings. 92*. Retrieved: http://aisel.aisnet.org/mcis2009/92
22. Den Bosch, J. van. (2021). Call of Duty Warzone players are being kicked from lobbies due to inactivity and they don't know why. *Esports.com*. Retrieved: https://www.esports.com/en/call-of-duty-warzone-players-are-being-kicked-from-lobbies-due-to-inactivity-and-they-dont-know-why-203572.
23. Denuvo (2021). Why game companies like Sony are using anti-cheat and anti-piracy technology (VB Live). *Venture Beat*. Retrieved: https://venturebeat.com/2021/06/17/why-game-companies-like-sony-are-using-anti-cheat-and-anti-piracy-technology-vb-live/
24. Derrington, S., Star, S. & Kelly, S.J. (2021). The case for uniform loot box regulation: a new classification typology and reform agenda. *Journal of Gambling Issues*.46. 302-332. DOI: https://doi.org/10.4309/jgi.2021.46.15.
25. Dey, D. (2021). FaZe Jarvis tries to stream Fortnite despite his permanent ban for a third-time, gets caught in 16 minutes. *Sportskeeda*. Retrieved: https://www.sportskeeda.com/esports/faze-jarvis-tries-stream-fortnite-permanent-ban-third-time-gets-caught-16-minutes
26. Duh, H. & Chen, V. (2009), Cheating Behaviors in Online Gaming, *International Conference on Online Communities and Social Computing*. 567-573. DOI: 10.1007/978-3-642-02774-1_61
27. Elchison, S. (2019). The Difference Between Esports & Gaming. *IPG Media Lab*.Retrieved:https://medium.com/ipg-media-lab/the-difference-between-esports-gaming-3bcb2d45d42b
28. Falcão, T., Marques, D.,Mussa, I.& Macedo, T. (2020). At the Edge of Utopia. Esports, Neoliberalism and the Gamer Culture's Descent into Madness. 13. 382-419.DOI: 10.26092/elib/411.
29. Freitas, B.D.A., Contreras-Espinosa, R.S., & Correia, P.Á.P. (2021). A Model of the Threats that Disreputable Behavior Present to Esports Sponsors. *Contemporary Management Research*, *17*(1), 27-64.
30. Fuentes, M.R., &Mercês, F. (2019). Cheats, Hacks, and Cyberattacks. *Trend Micro Research*. 8.
31. Georgiades, C. (2021). The Regulatory Landscape of Esports. *Money Smart Athlete Blog.* Retrieved: https://moneysmartathlete.com/2021/06/30/the-regulatory-landscape-of-esports/
32. Good, O.S. (2018). South Korea criminalizes 'boosting' with new law. *Polygon*,Retrieved: https://www.polygon.com/2018/12/9/18133391/south-korea-boosting-esports-league-of-legends-law
33. Haahr, M. (2017). Creating Location-Based Augmented-Reality Games for Cultural Heritage. *Joint International Conference on Serious Games.* DOI:10.1007/978-3-319-70111-0_29
34. Hallmann, K, and Giel, T, (2018) Esports – Competitive Sports or Recreational Activity? *21 Sport Management Review*.DOI:10.1016/j.smr.2017.07.011
35. Hamari, J. and Sjöblom, M. (2017) What is eSports and why do people watch it?.*Internet Res. 27*.211-232.
36. Hamstead, C. (2020), 'Nobody talks about it because everyone is on it': Adderall presents esports with an enigma. *The Washington Post.* Retrieved: https://www.washingtonpost.com/video-games/esports/2020/02/13/esports-adderall-drugs/
37. Hao, G. & Tan, D. (2021). Riot and Bungie band together against cheat creators by filing a lawsuit. *Dot Esports.* Retrieved: https://dotesports.com/business/news/riot-and-bungie-band-together-against-cheat-creators-by-filing-a-lawsuit
38. Henneberg, A.M. (2014). Anti-Doping Systems in Sports Are Doomed to Fail: A Probability And Cost Analysis. *4 Journal of Sports Medicine & Doping Studies.*
39. Hernandez, P.(2019). Popular Fortnite YouTuber permanently banned for cheating. *Polygon.* Retrieved: https://www.polygon.com/2019/11/4/20948032/fortnite-faze-jarvis-banned-aimhack-cheating
40. Heubl, B. (2020). Gaming - Hacking. When Cheating Leads to Crime. *15 Engineering &Technology*, 28-31. DOI: 10.1049/et.2020.0212
41. Hilvoorde, I. van, & Pot, N. (2016), Embodiment and Fundamental Motor Skills in Esports. *10 Sport, Ethics and Philosophy*. 1-14.DOI: 10.1080/17511321.2016.1159246
42. HLTV.org. (2021). 'KQLY Handed VAC Ban' *HLTV.org.*Retrieved:*https://www.hltv.org/news/13636/kqly-handed-vac-ban*
43. Holden J, Kaburakis A, &Rodenberg, R. (2017), The Future Is Now: Esports Policy Considerations and Potential Litigation, *SSRN Electronic Journal*
44. Hollis, L.P. (2018), Ghost-Students and The New Wave Of Online Cheating For Community College Students. *New Directions For Community Colleges 25*
45. Hollist, K.E., (2015), Time to Be Grown Ups About Video Gaming: The Rising Esports Industry and the Need for Regulation, *57 Ariz. L. Rev. 823, 833-34*
46. Huynh, M. &Valarino, F. (2019) An Analysis Of Continuous Consistency Models In Real Time Peer-To-Peer Fighting Games, *Hogskolan Kristianstad.*
47. Iwamoto, K. (1977). Go for Beginners. *New York: Pantheon*. ISBN 978-0-394-73331-9. 18.
48. Jacobs, H. (2015). Here's the Insane Training Schedule of a 20-Something Professional Gamer.*Business Insider*. Retrieved: https://www.businessinsider. com/pro-gamers-explain-the-insane-training-regimen-they-use-to-stay-on-top2015-5
49. Jasny, M. (2020). Doping in e-sports. An empirical exploration and search for sociological interpretations. *Acta Universitatis Lodziensis. Folia Sociologica*, (75), 93.

50. Kambhampati, A. & Star, S. (2021). Playing true? A critique of the 2021 WADA Code. *The International Sports Law Journal*. DOI: https://doi.org/10.1007/s40318-021-00193-z
51. Kanaan, M. (2020). T-Minus AI: Humanity'S Countdown To Artificial Intelligence And The New Pursuit Of Global Power. *Benbella Books.*
52. Kane, D. & Spradley, B.D. (2017). Recognizing ESports as a Sport. *The Sports Journal.* Retrieved: https://www.researchgate.net/profile/Daniel-Kane-6/publication/317929457_Recognizing_ESports_as_a_Sport/links/597f4db5a6fdcc1a9acd7fe1/Recognizing-ESports-as-a-Sport.pdf
53. Kedziora, M., Gorka, A., Marianski, A., &Jozwiak, I. (2020). Anti-Cheat tool for detecting unauthorized user interference in the unity engine using Blockchain. In *Data-Centric Business and Applications*. Springer, Cham. 191-209.
54. Kelly, S., Derrington, S. & Star, S. (2021). Governance challenges in esports: A best practice framework for addressing integrity and wellbeing issues. *International Journal of Sport Policy and Politics*. Forthcoming.
55. Lehtonen, S, (2020), Comparative Study Of Anti-Cheat Methods In Video Games, *University of Helsinki, Faculty of Science*.
56. Liu, S., & Jia, W. (2015), A survey: main virtualization methods and key virtualization technologies of CPU and memory. *The Open Cybernetics & Systemics Journal*, *9*(1).
57. Loria, K. (2016). Some Competitive Video Gamers are Abusing Drugs to get an Edge. *Business Insider*. Retrieved: https://www.businessinsider.com/esportsdoping-scandal-investigated-by-espns-otl-2016-1
58. Lozano, J.M, (2017), Video Games and Anti-Intellectualism: Higher Education In Modern Video Games *(2017) In: Tobolowsky B., Reynolds P. (eds) Anti-Intellectual Representations of American Colleges and Universities. Higher Education and Society. Palgrave Macmillan, New York.*DOI: https://doi.org/10.1057/978-1-137-57004-8_4
59. Macey, J., Tyrväinen, V., Pirkkalainen, H., &Hamari, J. (2020). Does esports spectating influence game consumption? *Behaviour& Information Technology*, 1-17.
60. Marquardt, A., Trepkowski, C., Eibich, T.D., Maiero, J., &Kruijff, E. (2019). Non-Visual Cues for View Management in Narrow Field of View Augmented Reality Displays. *2019 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*. 190-201.
61. Martinelli, J, (2018), The Challenges Of Implementing A Governing Body For Regulating Esports, *U Miami Int'l & Comp L Rev 26.*
62. Mauch, M.V. (2017). Why eSports are not recognized as a sport in Germany. *DW*. Retrieved: https://www.dw.com/en/why-esports-are-not-recognized-as-a-sport-in-germany/a-38188352
63. McCambridge, E. (2017). Anti-doping efforts still in their infancy in eSports. *DW*. Retrieved: https://www.dw.com/en/anti-doping-efforts-still-in-their-infancy-in-esports/a-39783790
64. McNeil, C. (2020). The Difference Between Cheating in Esports vs Traditional Sports. *EsportsTalk.* Retrieved: https://www.esportstalk.com/blog/the-difference-between-cheating-in-esports-vs-traditional-sports/
65. Michaeli, M, (2020), Grouping, In-Group Bias And The Cost Of Cheating, *121 Games and Economic Behavior*. DOI: 10.1016/j.geb.2020.02.002.
66. Mitchell, B. (2020). Guide to a Network Lag Switch. *LifeWire.* Retrieved: https://www.lifewire.com/what-is-a-lag-switch-817481
67. Nalli, J. (2019). Effect of esports and future development of esports. *Oulu University of Applied Sciences.* 1-31
68. Newton, D, (2018) Steroids And Doping In Sports: A Reference Handbook, *ABC-Clio. Santa Barbara (eds.),*ISBN - 978-1-4408-5481-1
69. Nunes, L.A.S., &Macedo, D.V.D. (2013). Saliva as a diagnostic fluid in sports medicine: potential and limitations. *JornalBrasileiro de Patologia e Medicina Laboratorial*, *49*. 247-255.
70. Paay, J., Kjeldskov, J., Internicola, D. and Thomasen. M., (2018). Motivations and practices for cheating in Pokémon GO. *In Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '18). Association for Computing Machinery, New York, NY, USA, Article 35*.1–13. DOI: https://doi.org/10.1145/3229434.3229466.
71. Parungo, N. (2021). Warzone: What Is Shadow Ban? *QFinity.* Retrieved: https://www.gfinityesports.com/call-of-duty-warzone/warzone-what-is-shadow-ban-ps4-ps5-xbox-pc/
72. Reis Cecin, F., de Oliveira Jannone, R., Resin Geyer, C.F., Garcia Martins, M., Barbosa, J.L.V. (2004). Freemmg: a hybrid peer-to-peer and client-server model for massively multiplayer games. In: *Proceedings of ACM SIGCOMM 2004 Workshops on NetGames'04. 172–172. ACM Press*
73. Rhodes, G.A. (2019). Waiting for the Augmented Reality 'Killer App': Pokémon GO. *In Augmented Reality Games I. Springer, Cham.* 3-14
74. Rietkerk, R. (2020), Why tapping into gaming should be top of mind for brands. *The Drum.* Retrieved: https://www.thedrum.com/industryinsights/2020/06/09/why-tapping-gaming-should-be-top-mind-brands
75. Rollinger, C. (eds.). (2020) Classical Antiquity in Video Games, First Edn,*Bloomsbury.*
76. Ruef, M. (2018). eSports - Professional Cheating in Computer Games. *SCIP*.Retrieved: https://www.scip.ch/en/?labs.20180906
77. Scholz, T.M. (2019). Unwritten Governing Principles. In eSports is Business. *Palgrave Pivot, Cham*. 101-116
78. Singh, V. (2021). Galaxy Racer Esports suspended coaching staff member until the claims are all addressed. *Inside Sport.* Retrieved: https://www.insidesport.co/galaxy-racer-esports-suspended-coaching-staff-member-until-the-claims-are-all-addressed/
79. Sparrow, L., Gibbs, M. and Arnold, M. (2019). Apathetic Villagers and The Trolls Who Love Them: Player Amorality in Online Multiplayer Games *In Proceedings of the 31st Australian Conference on Human-Computer-Interaction (OZCHI'19). Association for Computing Machinery, New York, NY, USA,* 447–451. DOI: https://doi.org/10.1145/3369457.3369514
80. Star, S. &Bakshi, N. (2019). The growth of esports in India – a short review of the main legal and regulatory challenges. *LawInSport.* Retrieved: https://www.lawinsport.com/topics/item/the-growth-of-esports-in-india-a-short-review-of-the-main-legal-and-regulatory-challenges.

81. Stavropoulos, A. (2020). Dashboarders demoted, receive adjusted ranked rewards in Apex Legends "Judgment Day". *Dot Esports.* Retrieved: https://dotesports.com/apex-legends/news/dashboarders-demoted-and-lose-ranked-rewards-in-apex-legends-judgment-day.
82. Stivers, C. (2016). The first competitive video gaming anti-doping policy and its deficiencies under European Union law. *San Diego Int'l LJ*, 18. 263.
83. Stubbs, M. (2020). 'Dota 2' Team Newbee Banned From Chinese Competitions For Match Fixing. *Forbes.*Retrieved: https://www.forbes.com/sites/mikestubbs/2020/05/15/dota-2-team-newbee-banned-from--chinese-competitions-for-match-fixing/?sh=220f85374dbe
84. The Fortnite Kid. (2021), Nick Eh 30 Caught CHEATING in $500k Fortnite Tournament! The Fortnight Kid.*YouTube*. Retrieved: https://youtu.be/DiWobtfjBLs
85. TheScore esports. (2020). From Banned to the Best: Shaiiko's Revenge Tour. *Whitehaven Journal*. Retrieved: https://journal.altervista.org/from-banned-to-the-best-shaiikos-revenge-tour/
86. Thomas, L. &Kadish, J. (2021). Playing with privacy? Privacy and cybersecurity considerations in esports. *Esports Insider*. Retrieved:https://esportsinsider.com/2021/06/playing-with-privacy-privacy-and-cybersecurity-considerations-in-esports/
87. Tomicic, I., Grd, P. &Schatten, M. (2019) Reverse Engineering of the MMORPG Client Protocol. *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*.1099-1104.
88. Torres, R. (2007). Win Trading: Cheating for the top Arena spots. *Endgadget.com.* Retrieved: https://www.engadget.com/2007-11-27-win-trading-cheating-for-the-top-arena-spots.html
89. Turton, W. (2017). How to hack a mouse to win millions at esports. *The Outline*. Retrieved from https://theoutline.com/post/2032/how-to-hack-a-mouse-to-win-millions-atesports?zd=1&zi=zk35gmm5.
90. Valentine, R. (2019). Fortnite cheat maker exposes professional player cheating in World Cup, *gamesindustry.biz.* Retrieved: https://www.gamesindustry.biz/articles/2019-04-16-fortnite-cheat-maker-exposes-professional-player-cheating-in-world-cup
91. Webb, S.D., & Soh, S. (2007). Cheating in networked computer games: a review. In *Proceedings of the 2nd international conference on Digital interactive media in entertainment and arts*. 105-112.
92. Weyandt, L.L., White, T.L., Gudmundsdottir, B.G., Nitenson, A.Z., Rathkey, E.S., De Leon, K.A., & Bjorn, S.A. (2018). Neurocognitive, Autonomic, and Mood Effects of Adderall: A Pilot Study of Healthy College Students. Pharmacy (Basel, Switzerland), 6(3), 58.
93. Witkowski, E. (2012). On the Digital Playing Field: How We "Do Sport" With Networked Computer Games. *Games and Culture*, *7*(5).349–374. DOI:https://doi.org/10.1177/1555412012454222
94. Xu, H. and Lyu, M. (2016), Assessing the Security Properties of Software Obfuscation.14*(5) IEEE Security &Privacy*. 80-83. DOI: 10.1109/MSP.2016.112.
95. Yun, S.M. (2019). A Comparative Overview of Esports Against Traditional Sports Focused in the Legal Realm of Monetary Exploitation, Cheating, and Gambling. *Cardozo Arts & Ent. LJ*, *37*, 513.