Bachelor's Thesis Computing Science

Cheating and anti-cheat system action impacts on user experience

Bryan van de Ven
s1024205

January 11, 2023

First supervisor/assessor:
Mairieli Santos Wessel

Second assessor:
Nils Jansen

Radboud University

Abstract

Cheating in video games has been a problem for a while, and can even lead to the downfall of a game if not dealt with (Duh & Chen, 2009 [3]). Although the technical aspects of cheats and anti-cheat systems are often discussed, research that discusses the issue from a player perspective is rare (Consalvo, 2007 [5]). In this thesis, we aim to contribute to the knowledge regarding player views on cheats and anti-cheat systems. We perform a literature review to discover 15 cheater motivations and 4 cheater deterrents, compiled from a list of existing literature on the topic of cheater motivations. We also conduct a survey to discover how players view cheats and anti-cheat systems, and discover some interesting points regarding the effects of game design on cheating tendencies and privacy on anti-cheat system actions. We discover that micro-transactions and unfairly distributed resources in games can potentially increase a player's tendency to cheat. In addition, we also discover that although the majority of players want cheaters to be punished, they do not want said punishments to go beyond preventing the cheaters from playing the game due to worries about privacy and possible harassment.

Contents

Chapter 1

Introduction

Video games are a popular form of entertainment, and just like in real life, not everyone tends to play fair. Cheating in video games has been a problem for a while, and can even lead to the downfall of a game if not dealt with (Duh & Chen, 2009 [3]). One way to combat this is by designing an anti-cheat system meant to detect and punish cheating automatically. However, not only do cheaters find ways around them (hackmag, 2016 [14]), they've also sparked their own controversies around privacy (Espenschied, 2007 [9] & Wilde, 2021 [27]). Although the technical aspects of cheats and anti-cheat systems are often discussed, research that discusses the issue from a player perspective is rare (Consalvo, 2007 [5]). In this bachelor thesis, we will investigate cheater motivations by compiling a list of motivations discovered through literature review. In addition, a survey will be conducted to gather player opinions on cheating and anti-cheat system actions. Combined, this will not only provide a generalized set of possible cheater motivations, but will also further validate them. In addition, it will provide some insight into what players think about what the anti-cheat systems do, rather than how they work.

1.1 Approach

Determining how players feel about cheats and anti-cheat systems is something that can't be done without employing some kind of survey to gather their opinions. In order to aid us in constructing good questions to put in our survey, it is important we perform some research to determine what earlier works have already discovered. We constructed the following research question:

- How do cheats and anti-cheat system actions impact user experience?

To make it easier to answer the research question, we can split it into three sub-questions:

1. Why do people cheat in online multiplayer games?
2. How do users feel when they cheat or when someone else cheats?
3. What do users think about the quality of- and punishments given by anti-cheat systems?

1.1.1 Sub-question 1

Figuring out why people cheat in online multiplayer games will provide some insight into a player's personality and environment, which could highlight certain flaws in the game itself or the anti-cheat system strategy. We will be collecting an assortment of existing literature on the topic of cheater motivations and analyze their contents to compile a list of possible cheater motivations and deterrents. This list will not only help us understand what the most common reasons are for people to cheat or not to cheat, but will also help us formulate interesting questions in our surveys for our participants to answer. These questions will then force the participants to think critically and potentially view the situation from angles they would otherwise not consider.
Some example motivations we expect to find based on common real life crime motivations are:

- Gaining something of value in real life, such as money or prizes.
- Gaining notoriety or status.
- Hoping to impress others by their performances.
- Progressing in the game, like levelling up characters and items, unlocking things, etcetera without having to spend hours in the game doing this legitimately.

Though we don't specifically look at cheater deterrents, it is possible that we will encounter some during the literature review. Some example deterrents we may find are:

- Fear of receiving punishment of some kind.
- Fear of losing access to their game account.

1.1.2 Sub-questions 2 and 3

Users may feel different towards cheats when they are the cheater as apposed to when someone else is cheating. Although one may expect that most users will have negative feelings towards other players that are cheating, it is possible that a user could forgive or tolerate a cheater under certain circumstances. However, when it comes to anti-cheat systems, it is a lot

harder to imagine what the general consensus is, if any exists at all.
In order to get an idea of how users feel about cheats and anti-cheat systems, we will be launching a survey and distribute it to participants. The survey will consist of three parts:

1. Demographics. The first part will serve to collect background information about our participants. It will also establish for how long participants have played online multiplayer games, and how often they play them on average. This will help to ensure that our participants can be considered as experienced users, increasing the confidence in the results.

2. Cheater scenarios. The second part will consist of a list of scenarios. Some scenarios have a cheater present, and the user will be asked to answer a few questions about the scenario. Other scenarios set up a certain game environment or condition, and the user will be asked to answer a few questions related to whether or not they would consider cheating in the scenario.

3. Anti-cheat system scenarios. The third part will again consist of a list of scenarios. Some scenarios will make the anti-cheat system do something, and the user will be asked to judge the scenario. Other scenarios will set up a certain game environment or condition, and the user will be asked to decide how the anti-cheat system should react in the scenario.

The remaining chapters of this thesis will teach the reader the background knowledge of cheats and anti-cheat system, summarize the discovered literature and analyze the survey results. The results will be compared to the literature and possibilities for further research will be discussed.

Chapter 2

Preliminaries

In order to better understand the cheating problem, some definitions and history will be explained in this chapter. Although we will briefly mention how cheats and anti-cheat systems work, the majority of the technical details will not be mentioned, as it is outside the scope of this thesis.

2.1 Cheats

Cheats in video games take on many forms, each serving a specific purpose. We will only consider cheats for online multiplayer games. Providing a definition for cheating is difficult, and many literately works tend to make their own definition. The biggest issue is that the people that can give the best definition of cheating are players. When players define cheats, they not only consider the game, but also the whole media system surrounding the game, which includes the player's subjective gaming experience, social meetings inside the game, and their personal value systems (Berger & McDougall, 2013 [1]). This means that every player makes their own definition of cheating. What one player sees as cheating, another may see as valid behavior. In this thesis, we do not adopt any particular definition of cheating, and instead investigated what definitions other people made. However, to aid the reader in understanding cheats, we will note that most definitions of cheating at least mention the following categories:

- Using additional code or software to modify the game.
- Abusing faulty code in the game without using additional code or software.
- Performing certain actions without using or altering code at all, such as looking at your friend's screen.

2.1.1 How do cheats work?

One of the most common ways that people cheat in video games is by using third party software that alters the game code. There are two main features of computers used by online games that most of these programs exploit: The Random Access Memory (RAM) and the online network.

Random Access Memory

The RAM is the place where a game stores its information, such as where on the map your character is located and how much health you have. Cheats can inject their own code into parts of the RAM to make the game behave differently. For example, an aimbot (see appendix A) can be implemented roughly as follows:

1. Find the location of an enemy in the RAM.
2. Set the position of the crosshair to face that enemy.
3. Fire a shot.

Wall-hacks and ESP (see appendix A) work in a similar fashion, getting the required data from RAM and then using that to gain an advantage.

Online network

Online games need a way for players to communicate with the server and with other players, for which it has to use the online network. The network is not always reliable, as anyone with the right skills can access and inspect the connections on their device. Just like how hackers can eavesdrop on regular information that travels around the web, cheat programs can eavesdrop on the game's communication on the web. This allows cheats to add, manipulate or destroy information travelling to and from the host device. One notable cheat that uses this is the latency cheat, also called 'Fake Lag' (see appendix A). It works as follows:

1. Wait for an enemy to show themselves.
2. Fire a shot at the enemy. This is sometimes also done with an aimbot.
3. Send a packet to the server stating that you were experiencing high ping.
4. The server registers a hit, even if the enemy is already back behind cover. This happens because the server tries to compensate for your 'lag'[1]. The cheat is an exaggeration of the 'peeker's advantage' problem (deWet & Straily, 2020 [6]) that all FPS games face.

[1]Lag refers to low framerate (bad game performace) or high ping (bad connection)

2.2 Anti-cheat systems

Anti-cheat systems serve a single purpose, namely to autonomously detect and punish cheaters. These systems can be implemented in various ways, but there is one critical choice that each implementation has to make: Will the system run on the server, or on the client? The chosen implementation will impact the strengths and weaknesses of the anti-cheat system, and is therefore a hard choice to make.

Server based systems

A server based anti-cheat system has the main benefit of being isolated from client systems, making it much harder for cheater's to alter or bypass the anti-cheat. The main drawback this implementation has, however, is that it is also harder for the anti-cheat system to detect more sophisticated cheats, as it does not have access to the client machine. In addition, running an anti-cheat system for a large player base comes with massive computation costs. The development and maintenance costs of anti-cheat systems can take up to 50% of a game's resources (Salen & Zimmerman [23]), and for a server based system, the resource cost will increase as the player base increases.

Client based system

The alternative choice of a client based system inverses the benefits and drawbacks of the server based system. Due to being on the client machine, the system has access the client machine and can therefore more effectively detect suspicious behavior of the client machine by investigating areas of the RAM, calls to other applications, etcetera. It also uses the client's resources to run the anti-cheat, freeing up resources on the server that can then be used to improve game performance instead of managing an anti-cheat system. However, being located on the client machine also means that clever cheat developers can manipulate or even completely avoid the anti-cheat system.

2.3 Cheats versus Anti Cheat Systems

Cheats are often purchasable as a subscription based service that includes the cheats themselves, support staff for helping with using and installing the cheat and community servers for communicating the status of the cheat's detection rates by anti-cheat systems. These subscriptions can go as high as several hundreds of dollars a month. The market for cheats will likely always exist as long as people are willing to put an 'enhanced' gaming experience above their wallets, and the potential financial gains for cheat developers

drives them to keep improving their cheats over time. This means that there may not be much we can do about demand, and can only really tackle supply by means of anti-cheat systems.

Unfortunately, not all games make use of anti-cheat systems, and games with fewer available resources tend to rely on free third party anti-cheat software like 'Easy Anti-Cheat' [11] and BattlEye' [16], which are both client based anti-cheat systems. Although this is still better than no anti-cheat at all, the software is publicly available and hence a skilled cheat developer can attempt to reverse engineer it to discover vulnerabilities they can use to circumvent the anti-cheat. Anti-cheat system developers attempt to mitigate this risk by not releasing details of how their systems work, operating by the concept of 'security by obscurity'. This concept poses a problem when we think about digital privacy, as we don't know what exactly the anti-cheat system is doing on your client machine.

Several years ago, most client based systems used to only have ring 3 privileges (Ellis, 2020 [8]) just like the majority of regular user programs. This lead to cheat developers creating cheats that ran in ring 0, also known as kernel mode. Programs running in this ring have full access to the system, and cheaters could use this to alter data that the anti-cheat system relied on, effectively rendering it useless. The solution to combat this sounds simple: Let anti-cheat systems also run in kernel mode. However, this solution has sparked plenty of discussions about privacy and security. Installing a cheat voluntarily that is owned by a single person or small group is quite different from being forced to install an anti-cheat system owned by a large company. However, probably the biggest problem with anti-cheat systems running in kernel mode is that there is no safety net when there is an issue with the anti-cheat system. A crash in a ring 3 program can at most cause the program that caused it to terminate unexpectedly, but no more than that. A crash in a kernel mode program can cause anything from a blue screen of death to complete corruption of important files, rending your device useless. Although most well known anti-cheat systems run in kernel mode nowadays, a relatively new anti-cheat system that really demonstrates the above mentioned issues is Valorant's Vanguard anti cheat system (Wilde, 2021 [27]). Vanguard could outright stop programs from running if it suspected it was a cheat program. In the open beta of Valorant, the anti-cheat's notifications of when it blocks a program weren't working well and the aggressiveness of the system was quite high. Since Vanguard is an always-on anti-cheat[2], this caused a lot of issues for players. This ranged from innocent things like mice and keyboards not working or programs like notepad not opening, to severe issues like device drivers used for cooling pc components being blocked and causing pc's to overheat. Hilariously enough, it took less than a month be-

[2] An 'always-on anti-cheat' is running regardless of whether or not the associated game is running

fore people had managed to bypass the system with cheats.

Nobody knows how long this tug-of-war between cheats and anti-cheat systems will last, or if it will even end at all. While anti-cheat systems are forced to become more and more intrusive to keep up with cheat developments, cheat developers have started to look at different approaches of cheating as well. Someone even managed to make a robot that can physically control the mouse using machine learning [12], making it almost impossible to distinguish it from a legitimate player. If such devices become common practice, anti-cheat systems may no longer be a viable strategy for protecting game integrity and it would be game over for the whole gaming community. With this in mind, perhaps it is time we re-investigate the demand side of cheats and explore what drives a player to cheat, and if there are ways we can mitigate those drives.

2.4 Summary

Defining what counts as cheating is difficult, since every player makes their own definition of cheating. In general, most definitions talk about game modifications, abusing faulty existing code or abusing other aspects that don't directly relate to the game. The first category, game modifications, can be used to detect the use of cheats. Though such systems will not catch all cheaters, they have forced cheat developers to improve their cheats to avoid detection. This in term forces the anti-cheat system developers to improve their system, which often can't be done without making it more intrusive. This is a cycle that has been going for a while now, with no signs of stopping anytime soon. Since their is a strong financial incentive for cheat developers, it is likely that they will continue to develop cheats that may become harder and harder for an anti-cheat system to detect. Since we can't easily force cheat developers to stop making cheats and cannot prevent cheating with anti-cheat systems, it may be time to start looking at different approaches. If we can somehow take away a players intention to cheat, then the financial incentive for cheat developers vanishes and the cycle would be broken. In order to do so, we must first understand not only what drives a player to cheat, but also to what extent an anti-cheat system can contribute to decreasing cheating tendencies. By doing so, we hope to find patterns in game design or player behaviors that we can use to take away certain cheater motivations, which in turn could reduce the amount of cheaters.

Chapter 3

Related Work

Before we introduce our own research, we will briefly look at what others have already studied regarding cheats and anti-cheat systems. This will show what the main methodologies are that have been used in earlier studies and shows what angles have been taken when viewing the cheating problem.

Blackburn [2] has done research into the effects of having cheater friends and has shown that having many cheaters as your friends can increase your own tendency to cheat. A similar study was conducted by Zuo et al [29], who analyzed data from several steam games and discovered that observing unpunished cheaters can also increase your own tendency to cheat.

Doherty et al [7] have interviewed undergraduate students, letting them take part in an experiment with three groups where each group has different opportunities to cheat. Each group was then asked to provide examples of when they cheated in the past, which were then sorted into 13 categories of cheater motivations.

Vázquez and Consalvo [25] have conducted several interviews to discover motivations for cheating in social network games. Since most of the games in this genre tend to be free to play games, different motivations arose that less are common in paid games. Paay et al [19] looked more specifically at one such game, namely the location based game 'Pokémon GO. Through several interviews, they identified motivations for cheating and encountered some forms of cheating not otherwise seen in other game genres, such as playing on several devices at once or taping a phone to a ceiling fan or other moving object.

Ribbens et al [22] have interviewed 256 participants, 13 of which in person and the remainder through an online questionnaire. Their sample groups consisted mostly of cheaters, resulting in a nice data set of cheater motivations. In addition, they also provide several examples of statements from respondents, allowing readers to identify the motivations themselves as well.

Sharma et al [24] have conducted a survey with 404 respondents. They mostly investigated the social motivations and influences of the respondents' ethical judgements, concluding that observing significant others cheating can increase the tendency to cheat. Similarly, Wu and Chen [28] also conducted an only survey, receiving 1374 responses with the majority having admitted to cheating in the past. The articles summarizes the discovered motivations and looks at some ethical aspects of cheating and the respondents' motivations.

Hardy [15] has written a master thesis where they studied the effects of being caught cheating on cheating in the future. Though they admitted that their experiments did not provide the exact results they were hoping for, it still provides interesting points to investigate in further research.

Chen and Ong [4] used focus groups to interview 29 participants to not only determine possible motivations for cheating, but also to discover how they define cheating. The article sheds light on some aspects players take into account when defining cheating.

The vast majority of the related works above use surveys or interviews as their main methodology for their research. Each work has their own categories of cheater motivations, and although most of them do mention motivations found in other related works, they are all individual studies. Our research aims to combine the knowledge of these works to establish which motivations were discovered, and count how often each motivation was discovered independently. In addition, we will contribute to this by performing our own survey to add to this knowledge base. Though it would also be interesting to count how often a motivation was given by all participants combined from all of the related works, this is not possible since not all sample data is publicly accessible and since there would be no way to know whether each participant is unique or has participated in multiple works. Finally, since none of these studies dive into how anti-cheat systems could influence cheater tendencies and little research exists regarding the effects of anti-cheat systems on user experience, we will investigate this using our survey as well.

Chapter 4

Literature review

4.1 Methodology

A literature review was conducted to answer sub-question 1 (see section 1.1.1). This was done using Google Scholar over a period of about a week. The exact query used was '*why do people cheat in online multiplayer video games*'. No sorting conditions were applied, as sorting conditions can subtly change the input query. Only the first 10 pages of results were used in the literature review, with each page having 10 results and thus yielding a total of 100 results. Since the review spanned multiple days, the order of articles changed slightly over time. In an attempt to mitigate this, each day the literature review was conducted would start by going over all previously completed pages to scan for shifted results. Any results that had made their way higher up the list into completed pages would then also be considered for the literature review. In the end, only 97 results were subjected to the literature review process, as there were a few duplicate results that led to the same article.

Stage 1

In the first stage, all results were subjected to the following inclusion criteria:

- The language used must be English.
- Must be about cheating in multiplayer online video games. This means that offline or singleplayer games are discarded.
- Primary focus must either be about the reasons people cheat or be about things that encourage or discourage cheating.

During the literature review, two lists were used to keep track of which results were usable and which weren't. For each result, we would read the abstract first and then apply the criteria. Anything that met all inclusion

criteria was included in the 'valid results' list, whereas anything that did not was included in the 'invalid results' list along with the main reason for discarding it. This provided a good overview of what results had already been covered. At the end of this stage, we had 11 results on the 'valid results' list and 86 results on the 'invalid results' list.

Stage 2

In the second stage, everything on the 'valid results' list was downloaded as PDF and then read in full. During this process, the highlight feature of the PDF editor in Microsoft Edge was used to highlight information in the text that would be useful to us. We could then save the article and it would keep the highlights, which made it easier to find the information whenever we needed it. The highlight color scheme we used was as follows:

- Yellow: Game genres and game titles.
- Green: Cheating motivations and deterrents.
- Blue: Data used or generated by the literature.
- Pink: References to possible other literature or quotes.
- Red: Miscellaneous, such as problem definitions or useful facts.

During this process, we had to remove one more articles from the list, as it did not have usable information in it despite passing the inclusion criteria. This left us with a total of 10 articles we could use. The full list of articles can be found in section 3.

Stage 3

In the final stage, the information discovered in the articles was compiled into an Excel file. This file consisted of six sheets: One for each of the color categories mentioned in stage 2 and one for summarizing the cheater motivations and deterrents. We should note that we only included motivations and deterrents that the article authors themselves had discovered through their own experiments, surveys, etcetera. We left out any motivation and deterrent that was cited as being discovered by someone else, as we only wanted to include reasons that were backed up by data and personally discovered by the authors.

4.2 Results

Compiling the list of cheater motivations and deterrents turned out to be slightly more challenging than expected. In an effort to condense the list,

motivations and deterrents that were similar were combined into one category. An example of this is the combination of 'The game is not competitive', 'It's just a game' and 'Cheating is fun' into one category 'Not competitive / Not serious / Fun'. Although we could also further condense that category into just 'Not serious', we decided to keep a few of the most commonly mentioned aspects of the category in the title to explicitly show that we merged those reasons into one category.

In the end, we discovered 15 cheater motivations and 4 deterrents (see figure 4.1). Although some reasons like 'technical issue' were unexpected, all of them do make sense and are understandable reasons. Interestingly enough, all four deterrents were also used as motivations, indicating that there is some duality to reasons. One player might use a particular reason to justify cheating, whereas another may use the same reason to explain why they don't want to cheat.
The three most common motivations were 'Other cheaters', 'Not competitive / Not serious / Fun' and 'Social bonding'. The three most common deterrents were 'Punishment', 'Other cheaters' and 'Financial'. Since we only focused specifically on cheater motivations in the literature review, it is not surprising that we only discovered 4 deterrents as opposed to the 15 motivations we found.

Cheater motivations

For each of the cheater motivations, we provide a generic description and examples of how it is used to justify cheating. These descriptions and examples were carefully crafted based on the descriptions and actual data and responses from the articles in the literature review.

- Progress: Used when stuck in a game, tasks are repetitive or boring, etcetera. Sometimes games can be difficult or have recurring tasks that eventually get boring to do by hand. This can cause people to start cheating to progress further in the game without putting in effort themselves.

- Gain advantage / Compensation: Used to make it easier to win, make up for a lack of skill or when facing tough opponents. Often used when people simply like to win or feel like they are worse than the other players and want to make up for that.

- Gain resources: Used to gain items without putting in the work. Tends to be used in games that require the player to collect resources to progress. Although similar to the 'Progress' category, it was deemed different enough to have its own category.

Item	Times mentioned as motivation	Times mentioned as deterrent	Times mentioned as both
Progress	4	0	0
Gain advantage / Compensation	4	1	1
Gain resources	1	0	0
Keep appearance / Social status	2	0	0
Emotional	1	0	0
Technical issue	3	0	0
Help others	3	0	0
Alter gameplay	4	0	0
Financial	4	1	1
Other cheaters	6	1	1
Punishment	2	2	1
Not competitive / Not serious / Fun	6	0	0
Annoy others	1	0	0
Social bonding	5	0	0
Curiosity	2	0	0

Figure 4.1: Overview of cheater motivations and deterrents

- Keep appearance / Social status: Used by people that enjoy having a status as 'good player' or not wanting to look bad to their teammates or friends.

- Emotional: Used by people experiencing heavy emotions like anger or sadness. Although one may deem this to not be a valid justification for cheating, life has shown plenty of examples of crimes committed in a fit of emotional rage and as such this is not a surprising motivation.

- Technical issue: Used when there are faults in the game's design, such as bugs or inherently broken features that cause unfair advantages and disadvantages. An example of the latter are location based games that reward lots of movement, which causes an unfair disadvantage for people unable to move regularly. This group of people isn't limited to just people bound to a wheelchair or suffering a broken leg, but extends to people with little free time due to other social obligations or even just people that can't go outside due to a long lasting weather condition.

- Help others: Used to justify cheating in the name of the greater good. Although it is still cheating and may still impact other players in a competitive game setting, this motivation is often used to justify cheating in a co-op setting with the intention of helping fellow players succeed in their goals.

- Alter gameplay: Used when people want a different game experience in the game than that game normally offers. This ranges from simple things like making the game more or less challenging, to more elaborate things like enabling people to make their own stories and role-play in the game.

- Financial: Used when in-game items can't be afforded by the cheater, or when attempting to gain money from cheating by selling self-made cheats or manipulating data in events with prize pools to sway the results.

- Other cheaters: Used to justify cheating because other players are also cheating. Some players use this motivation to cheat because there are too many other cheaters in the game to stand a chance at winning without cheating yourself. Another type of player uses this motivation to justify cheating to mitigate the impacts of another cheater as a way of fighting fire with fire, and only use cheats for this particular reason.

- Punishment: Used when a player perceives a lack of punishment for disallowed behavior in the game, but often as a secondary motivation. A lack of an anti-cheat system can encourage players to cheat as

observing cheaters go unpunished can encourage cheating (Zuo et al, 2018 [29]).

- Not competitive / Not serious / Fun: Used when people don't take the game seriously or when they don't have any other clear reason for cheating besides doing it for fun.
- Annoy others: Used by players who like being annoying and seeing the frustrated reactions they get from the other players. Although rarely used as primary reason, several data responses in the articles we reviewed did mention cheaters liking the reactions even if those weren't their main goal.
- Social bonding: Often used by cheaters playing with close friends or family members as a way to socially bond. It is quite similar to the 'Fun' category, but has a different end goal and therefore received its own category.
- Curiosity: Used by people that are simply curious about how a cheat works, or how the game code interacts with it as a way of finding out how the game works and where its strengths and weaknesses lie.

Cheater deterrents

For each of the cheater deterrents, we provide a generic description and examples of how it is used to justify cheating. These descriptions and examples were carefully crafted based on the descriptions and actual data and responses from the articles in the literature review.

- Gain advantage / Compensation: Cheats can give you an advantage or compensate for skill differences. This can lead to feeling a loss of challenge, making the game boring to play.
- Financial: Cheats can be very expensive, and not everyone is willing to invest a lot of money into them. In addition, punishments can cause a loss of your account. Not only do you thereby lose the money spent on buying the account, you also lose any money you spent on micro-transactions in the game.
- Other cheaters: As a game has more cheaters in it, players may feel that the odds of being caught also increase, especially if the game has a report feature or anti-cheat system. Some players may choose to not cheat in that particular game because of this imagined higher risk of being caught.
- Punishment: The most obvious deterrent of all, being punished for cheating can deter players from cheating. Punishments range from

small punishments like muted accounts or temporary bans to permanent bans, IP bans and hardware bans, and tend to increase in severity as the number of prior offences increases.

4.3 Final considerations

With the lists of motivations now constructed, we can attempt to deduce which of the items are likely to occur in which games, and which items could potentially be mitigated. First of all, it should be obvious that any game with a competitive nature is automatically subject to the 'Gain advantage / Compensation' motivation. It is also easy to see that some motivations like 'Curiosity' and 'Not competitive / Not serious / Fun' can be present in any game, as these have nothing to do with the game itself. As such, these are motivations that cannot be mitigated by anyone other than the cheater itself. Some other motivations like 'Progress' and 'Gain resources' can be reduced by avoiding making repetitive tasks in games and by only requiring very little resources to be collected for progress. However, this would remove a lot of popular games and fun mechanics, and is therefore not always the best action to take. Another way to deal with these could be to offer players a free boost when they're stuck somewhere for a certain amount of time, though this could take away some fun and replay-ability and perhaps even cause players to purposely wait for these free boosts instead of actually playing the game. Other motivations that are easier to deal with are 'Punishment' and 'Other cheaters', which can be dealt with using anti-cheat systems. Though these systems are often far from perfect, a lack of these can severely increase the amount of cheaters in a game. Finally, there may be ways to deal with motivations like 'Emotional' and 'Curiosity'. Giving players that lose repeated matches or encounter cheaters a motivating message in-game could help boost their morale and calm their emotions. Similarly, displaying messages on occasion about the harms that cheating can cause may reduce curiosity, though some players may be annoyed by the messages.

Chapter 5

Survey

5.1 Methodology

Since sub-questions 2 and 3 (see section 1.1.2) deal with exploring a user's feelings towards cheats and anti-cheat systems, we conducted a survey to gather those feelings. We started by constructing a pilot survey with Qualtrics [21] using the results from the literature review as inspiration for constructing interesting questions and as guidelines for important information to gather in the demographics. This pilot survey was sent out to a small group of friends that were known to be avid gamers. The pilot survey was closed after 7 responses were gathered, and then the feedback was used to improve the survey. Afterwards, the improved survey was distributed via discord game servers, personal friend groups and colleagues of my supervisor that had shown interest in participating. The survey ran for approximately 52 days, and received 17 responses during that period. Out of those 17 responses, 3 were completely blank and 1 had abandoned the survey early on, leaving us with a total of 13 valid responses. We are unsure whether the blank responses were system errors or people that closed the survey without answering anything at all.

5.2 Results

For your convenience, we separate the results into three sections matching the structure of the survey: demographics, cheater scenarios and anti-cheat system scenarios. In all results, the four unfinished responses were filtered out. In order to avoid cluttering the thesis, most of the figures referred to in this section can be found in appendix B. The results include exact statements given by participants, with only minor spelling or grammar mistakes having been manually fixed by us.

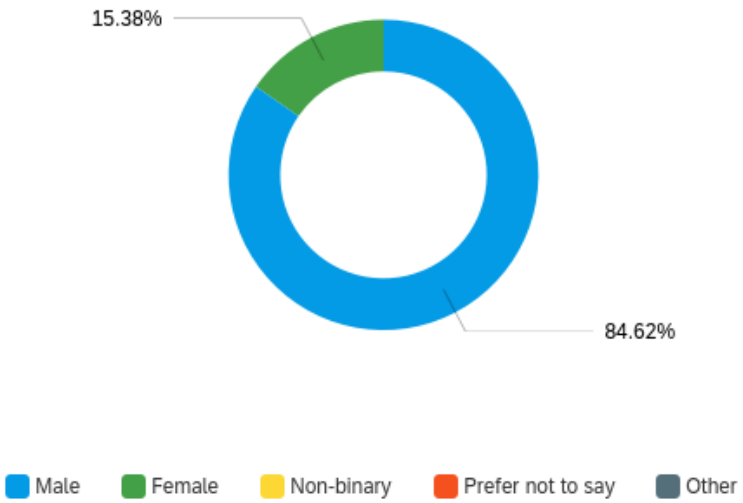

Figure 5.1: Gender distribution

5.2.1 Demographics

The age of the participants ranged from 18 to 34 years, with an average age of roughly 27. Most of our participants were male, with 11 out of 13 answering male and 2 out of 13 answering female (see figure 5.1). The vast majority of the participants have played online multiplayer video games for more than 5 years and play at least once a month (see figure 5.2 and B.1). Despite the low amount of participants, this make us feel confident that we have an experienced sample group. It should be noted that one participant replied that they don't play online multiplayer games. However, since their answers to other demographic questions heavily imply that they do in fact play online multiplayer games, we presumed this was accidentally answered incorrectly. The most popular game genre amongst the participants was FPS [1] with 92% of the participants playing this genre (see figure 5.3). Four participants wrote down additional genres using the provided text box. This yielded the following additional genres: Sport, Co-op, Sandbox, Survival, Asymmetrical horror, Tower defense and Racing. None of those participants wrote down the same additional genre, giving each one a selection rate of about 7.7%. The three most played games were Overwatch 2, League of Legends and Counter-Strike: Global Offensive (see figure B.2). Despite instructions to only include online multiplayer games, some participants also included singleplayer games. These singleplayer games have excluded

[1] First Person Shooter

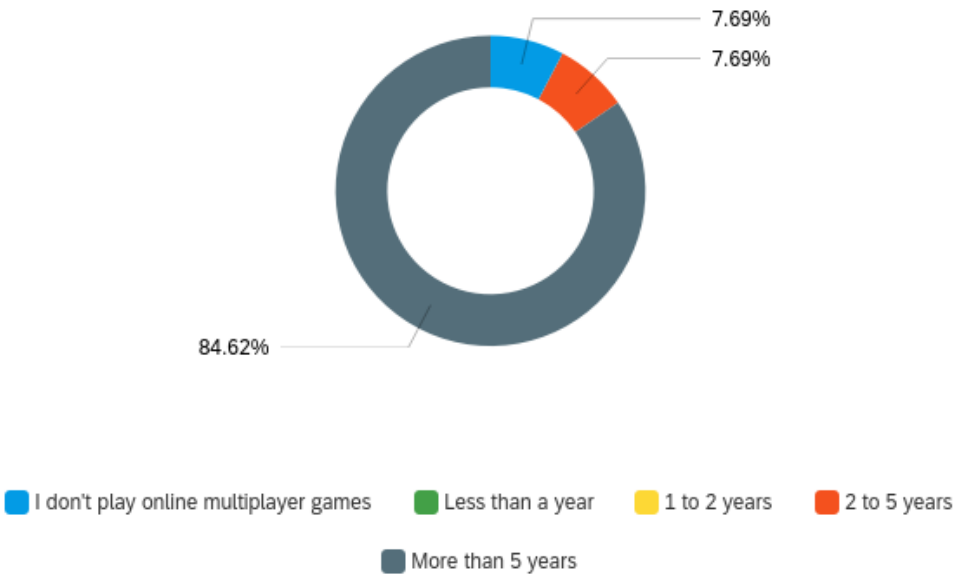

Figure 5.2: Period of time where participants have played online multiplayer games

from the results. Two of the participants stopped playing one or more of their selected games due to cheaters, with one having stopped playing Apex Legends and CS:GO, and the other not having specified which game exactly they stopped playing.

We asked our participants how they would define cheating, and to use their definition when answering the remaining questions of the survey. Out of the 13 participants, 8 participants mentioned 'gaining (unfair) advantage' in their definition of cheating. Unfortunately, due to the open nature of the question, most participants did not mention exactly what they considered cheating. As an example, P4 (Participant 4) defined cheating as "*Anything that the game mechanics don't allow players to do.*", which is open to interpretation. Another definition of cheating given by P6 is "*Using methods outside of the actual game mechanics to get an advantage in a player vs player situation. I would for example also consider exploiting glitches as cheating if it is done to gain an advantage over another player.*". Although this definition is already clearer than P4's definition, it is still not concrete, as P6's definition seems to deem abusing glitches as cheating if it is done to gain an advantage, but not as cheating if done for any other reason. Perhaps the question should have been rephrased to allow participants to form a clearer response.

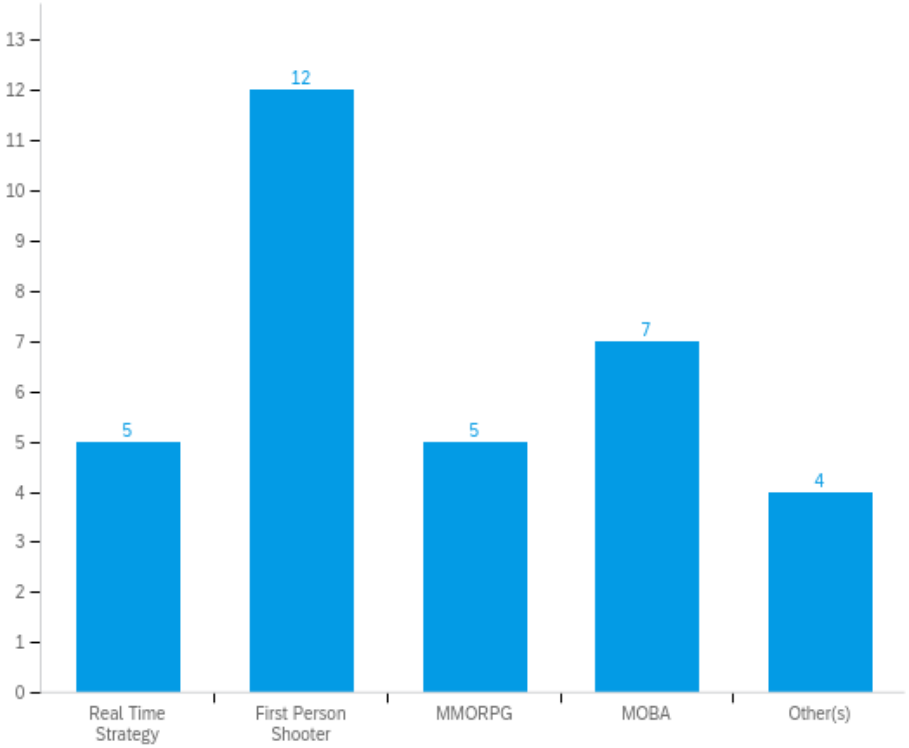

Figure 5.3: Game genres played by participants

Although it can sometimes be hard to concretely prove someone is cheating, many games can spot cheaters by observing suspicious behavior. Therefore, we also asked how often participants felt like they encountered cheaters in their matches. Even though this is a subjective guess on their part, it is still an interesting question to ask. Roughly 38.5% of the participants answered that they encounter a cheater in 1 out of every 50 matches they play (see figure 5.4). Surprisingly, about 53.9% of participants answered with less than 1 out of every 100 matches they play. This could suggest that perhaps the cheater problem is decreasing in severity. However, we must remember that our sample group consisted of just 13 participants and hence the sample size is too small to draw a definitive conclusion.

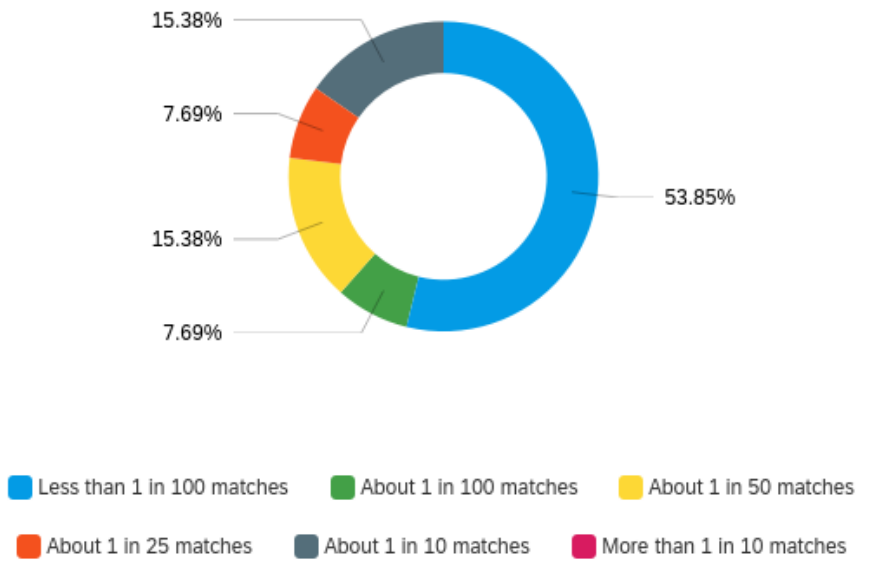

Figure 5.4: Cheater frequency guesses

In our sample group, 2 participants admitted to cheating (see figure B.3), with P2 answering 'always' and P3 answering 'sometimes'. Both of them provided 'Fun' as their single motivation for cheating, which is one of the 3 most common categories we discovered in section 4.2.

5.2.2 Cheater scenarios

The cheater scenarios were divided into two parts. The first three questions were carefully designed to make the reader question their own reasoning. They each presented a cheater in a certain scenario, and asked the reader to give their judgement. Scenario 1 asked the participant to judge a cheater

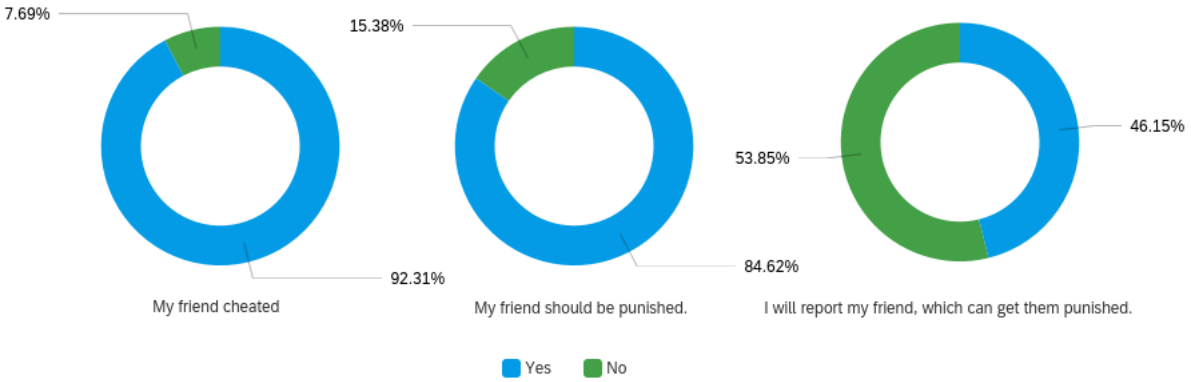

Figure 5.5: Scenario 3: Best friend is cheating

with high ping[2] who they observed cheating. Only about 46.2% of the participants deemed it unacceptable, with the remainder either not seeing it as cheating or forgiving the cheater (see figure B.4). Two answers given by participants are: "*Cheating is cheating ...*" (P12) and "*Why should I be penalized for his bad internet. There are other ways of dealing with high ping, and resorting to cheating is taking the 'nuclear option' if you ask me.*" (P7)

Scenario 2 asked the participant to judge a cheater (Cheater B) that prevents another cheater (Cheater A) from influencing the match. Once again, only about 46.2% of the participants deemed it unacceptable (see figure B.5). Roughly 30.8% of the participants explicitly answered that Cheater B should not be punished for cheating, indicating that some players may be sympathetic towards 'good' cheaters. P12 answered "*Previous answer, some games are just lost in spawn and thats how games are. No need to lower yourself to their level.*", whereas P1 answered "*Counter-cheating a cheater is fine, because they breached the whole premise of having a fair game*".

Scenario 3 is perhaps the most interesting scenario. It asks participants to judge their best friend as the cheater in the scenario. Although 84.6% of the participants want their friend to be punished for cheating, only 42.6% of the participants would report[3] their friend (see figure 5.5), indicating that the social bond is more important than the game integrity. We found this to be quite nice, as it shows that most players will put friendships above games. P8 had this to say: "*While my friend should be punished for cheating, I will not report them myself. For me, a good relationship with my friend is more important than some online game. ...*"

[2]High ping indicates a bad connection to the server

[3]Reporting a cheater increases the odds of them being considered for manual evidence reviews, increasing odds of being punished.

The remaining four questions were intended to gauge what game design elements and personal motivations would cause a participant to consider cheating. Scenario 4 presents a tournament with several mini scenarios taking place during the tournament. In all but two mini scenarios, at least 10 participants answered that they are very unlikely to cheat in the tournament (see figure B.6 and B.7). The only two mini scenarios where this was lower were the last two scenarios, which were also the only ones that have a cheater already present in the tournament. In these scenarios, 7 and 9 participants answered with 'very unlikely' respectively. This lower amount could be explained by 'Other cheaters' being one of the three most commonly mentioned motivations for players to cheat. Another interesting observation is that one participant answered all but one mini scenario with 'very likely' (P2). The only mini scenario where they answered differently is the scenario were all other players are friends of the participant. In that mini scenario, they answered 'neutral'. They did not provide any reasoning for this, so we can only assume that perhaps they do see friendship integrity as somewhat more important than cheating.

Scenario 5 was inspired by issues discovered in a research article regarding Pokémon GO (Paay et al, 2018 [20]), where it was observed that players would cheat due to the game giving advantages to people in crowded places. Scenario 5 taps into this issue, presenting the player with a game where certain resources are required for progression. Players are placed into one of three zones, with each better zone giving a higher amount of said resources than the zone below. Being placed in a higher zone did seem to slightly reduce the temptation to cheat (see figure B.8), though the sample size is too small to say for sure. P8, who answered 'very unlikely' everywhere in this scenario, explains their choices as follows: "*If I like the game mechanics, I will play the game as it's intended. If I don't like them, I would stop playing. I don't see a reason to cheat.*". Since only the participants that answered 'very unlikely' gave their motivations, we don't know the reasoning behind the choices of the other participants that selected other answers.

Scenario 6 was intended to discover if micro-transactions have an impact on the tendency to cheat, as these are becoming more common in games nowadays. Scenario 6 sets up a game where items can be bought from the developers with real money, and the participants are asked to answer a few questions. When the items are affordable or do not give real advantages for players that buy them, over 76.9% of the participants say that it's very unlikely that they'll cheat (see figure B.9). However, once the items become unaffordable or give severe advantages, this drops down to at most 61.5%, indicating that micro-transactions could potentially influence cheating tendencies. P1 said "*Pay to win*[4] *is a bit like cheating to*

[4]Pay to win refers to games where spending real life money increases your odds of

begin with", whereas P12 says "*Pay 2 win does suck, however I don't think I would cheat, I'd rather just avoid the genre.*". This seems to indicate that micro-transactions could not only increase cheating tendencies, but could also outright cause players to avoid the game altogether. Though the latter is out of scope of this thesis, it is an interesting thought.

Scenario 7 is intended to measure how effective an anti-cheat system is at deterring cheaters, and serves as a good transition point between the two scenario types. It sets up a game where the percentage of cheaters caught is known, and asks the participants to indicate whether they would consider cheating given those percentages. The results were inconclusive (see figure B.10), likely due to our sample group consisting of mostly 'fair' players. A sample group with a larger portion of cheaters, or perhaps only cheaters, would have been better for this scenario. It should be noted that P2 and P3 were the only participants that answered that they would cheat even if at least 75% of cheaters is caught by the anti-cheat system. These were also the only two participants that admitted to cheating, suggesting the possibility that some cheaters are not deterred by anti-cheat systems. A similar conclusion was also drawn in an earlier study in China by Wang et al [26]. Another observation comes from P1, who said "*More importantly, I would consider cheating if the percentage of cheaters is greater than some baseline.*". This is an interesting point that we had not considered before, and could have formulated a better question to use for this scenario. Instead of using the percentage of cheaters caught, we could have used the percentage of the player base that cheats. This would then likely divide the participants into two groups, namely those who would be tempted to cheat and those who'd rather not play the game in question at all.

5.2.3 Anti-cheat system scenarios

The anti-cheat system scenarios consisted of five questions designed to measure how participants want the anti-cheat systems to operate. Scenario 1 deals with information control, and asks the reader what information should be handed out when a cheater is caught by the anti-cheat system. With the many concerns of online privacy going around the past few years, it comes as no surprise that the majority of the participants do not want other players to receive the cheater's username or punishment history (see figure 5.6). When it comes to the cheater's punishment or detected cheats, the group is divided. Roughly half of the participants want other players to receive the information, whereas the other half does not. P4, who is part of the first group, explains their reasoning as follows: "*Anonymized info about what cheats are used and what punishment they got are interesting to see, and perhaps deters others from cheating.*". P7, who is part of the second group,

winning, often by buying strong items or perks not otherwise available.

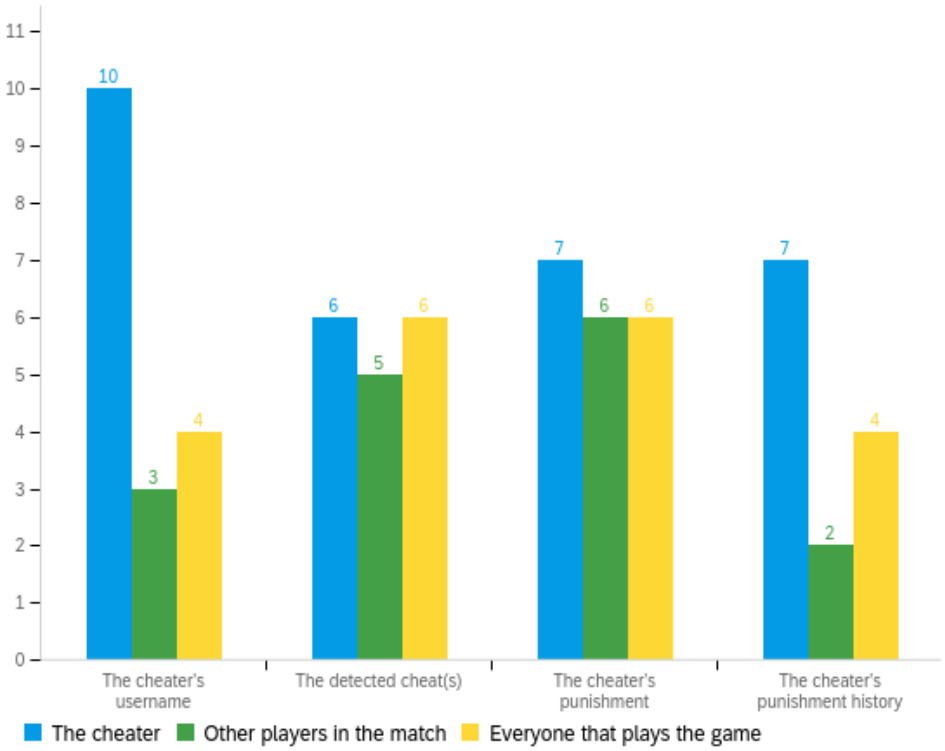

Figure 5.6: Scenario 1: Who should get what information when a cheater is caught?

explains their reasoning as follows: "*I feel like cheaters shouldn't be punished more than being unable to play the game. Giving out any more information than that serves no purpose other than putting the cheater at risk of being doxxed or harassed.*". Though both sides provide valid points, most games are part of the second group where only the cheater receives the relevant information, albeit useally without the detected cheat being revealed.

Scenario 2 asks participants what the anti-cheat system should do with a cheater it catches. As expected, the vast majority of the participants want the cheater to be removed from the match immediately (see figure B.11).

Scenario 3 aims to determine what participants would like to happen to a match where the anti-cheat system removes a player for cheating. We allowed participants to answer this scenario both from an uncompetive perspective and from a competitive perspective[5]. For competitive matches, the consensus seems to be to either reset or cancel the match without adding another player (see figure B.12 and B.13), whereas for uncompetive matches it seems preferred to add a new player and either add extra time to the match

[5]Competitive matches involve ranks, influenced by winning and losing. Uncompetitive matches don't involve ranks, and are meant for more relaxing experiences overall.

or reset it. P8 explains this difference well: "*In non-competitive matches, it is more fun to finish games. In competitive matches having a cheater against you is unfair, so the match should be canceled without penalties plus maybe a bonus for both teams (except the cheater of course) for the inconvinience*".

Scenario 4 deals with determining what punishments an anti-cheat system should be allowed to dish out to a caught cheater. There seems to be a consensus that it should not be allowed to do anything more severe than a short temporary ban, as only 3 to 5 participants selected the four most severe punishments (see figure B.14). The three mildest punishments were selected by 7 participants each. Two explanations given by P12 and P3 respectively are "*HWID*[6] *bans are really intrusive and should only be done to repeat offenders, cheating lists and or a perma ban is good though.*" and "*A cheater always find a way to return, no matter what. No need to ban.*". P3's explanation is especially intriguing, since they are one of the two participants that admitted to cheating. They selected the 'cheating list' and 'muted account' punishments as the only two punishments allowed. This poses an interesting strategy of tricking cheaters into thinking they haven't been caught, when in reality they've been playing against other known cheaters the entire time. Even when they find this out, they still have to decide whether they want to buy a new account to play against other people again. Since their own account technically still works, this could persuade them to stay on that account, protecting the community from them for a little longer.

The final question participants were asked was inspired by Valve's anti cheat (VAC) used in many Steam games. Cheaters caught by VAC receive a permanent 'VAC ban' marker on their account that is publicly visible. Participants were asked whether cheating accounts should have such a publicly visible indication or not. Nine participants answered no, three answered yes and one abstained. P7 explains why this indication should not exist: "*Valve does this with VAC. I don't think this should be the case, seeing as it permanently brands and shames the account for cheating. Maybe it was a one time offense, and the player learned their lesson? No need to permanently humiliate someone for making a mistake once.*". Several participants commented that the indication should not be given to first time offenders, but that multiple offenses could cause it to appear: "*No, not for 1 time cheaters, perhaps when they have been caught multiple times it's an option. And it should go away over time again.*" (P4). This shows that despite most participants condemning cheating, they do not want punishment to go beyond preventing the cheater from playing the game. It indicates a sort of moral high ground, where despite potential name calling during match chat, they do not actually want cheaters to be harassed or humiliated.

[6]Hardware Identification

5.3 Final considerations

It has become clear from our survey results that despite the majority of our participants being against cheating, there are circumstances where they are sympathetic with a cheater and can forgive them. We have seen that certain game design choices like micro-transactions or unfairly distributed resources may increase cheating tendencies, which lines up with motivations like 'Financial' and 'Technical issue' that we found in section 4. We've also discovered that most of our participants find privacy important, and do not want any information generated by an anti-cheat system to be given to anyone other than the player it pertains to. Finally, they also do not want punishments to go beyond preventing a cheater from playing the game, as more intrusive punishments could lead to a cheater being harassed or publicly humiliated.

Chapter 6

Conclusions

We have determined through literature review that there exist many reasons for someone to cheat. We compiled a list of 15 motivation categories and discovered some unexpected motivations. Cheating because of other cheaters, for fun or as a way of social bonding were the three most common motivations for cheating we discovered. Perhaps the two most interesting motivations were cheating to mitigate a technical design flaw or out of sheer curiosity. Though we were not looking for deterrents, we did find four of them as well. These were all also on the motivation list, suggesting a duality where some reasons can serve as both motivation or deterrent. Two participants in our survey admitted to cheating for fun, which is one of the most common motivations we found. Our survey results highlighted the fact that players all have their own definition of cheating, as Berger and McDougall have discovered before [1]. It also showed that despite most participants being unlikely to cheat no matter the circumstances, they do sympathize and understand other cheater's motivations in certain scenarios. The most notable result obtained was that over half of the participants would not report a friend as cheater, despite the majority wanting them to be punished for cheating. This shows that social bonds are valued higher than game integrity. It was also discovered that certain game mechanics like unfairly distributed resources or micro-transactions may influence the tendency to cheat, though our sample size is too small to say for sure. Furthermore, we also discovered that participants seem to care a lot about privacy, with less than half of the participants wanting the anti-cheat system to hand out information to anyone other than the player it pertains to. It also seems that perhaps there should be some difference between how the anti-cheat system affects competitive matches versus uncompetitive matches when it removes a cheater. Most games will terminate any type of match when a cheater is caught, however, our survey results show that most participants prefer an uncompetitive match to receive a new player and either continue with extra time or reset. We also found that the majority of participants do not

want anti-cheat systems to punish cheaters with anything more severe than a short, temporary ban. The motivations behind this seemed to be rooted in privacy concerns once again. Finally, we also saw that the majority of the participants are against public indications on cheating accounts, mainly for fear of those accounts being subject to harassment. This shows that despite most participants condemning cheating, they don't want cheaters to be harassed or humiliated and only want them to be prevented from playing the game.

We should note that our research is subject to some limitations. The literature review process is based on the unknown sorting nature of Google Scholar, and therefore it is possible that other important literary works were missed simply due to being further down the list. Moreover, we are dependent on the motivations listed in the included works. Since some works focused on more specific aspects of cheater motivations, it is possible that the ranking of the cheater motivations we discovered was influenced by the literary works we included. Finally, since our survey sample size consisted of just 13 participants, it is hard to make any concrete conclusions about our survey results. Conducting a similar survey with a larger sample size could be interesting in future research. We also believe more research should be conducted into how players view the anti-cheat system, as we discovered some interesting aspects that need to be explored further.

Bibliography

[1] Richard Berger and Julian McDougall. Reading videogames as (authorless) literature. *Literacy*, 47(3):142–149, 2013.

[2] Jeremy Blackburn. An analysis of (bad) behavior in online video games. 2014.

[3] Henry Been-Lirn Duh & Vivian Hsueh Hua Chen. Cheating behaviors in online gaming. In A. Ant Ozok and Panayiotis Zaphiris, editors, *Online Communities and Social Computing*, page 567–573. Springer Berlin, Heidelberg, 2009.

[4] Vivian Hsueh Hua Chen and Jeremy Ong. The rationalization process of online game cheating behaviors. *Information, Communication & Society*, 21(2):273–287, 2018.

[5] Mia Consalvo. *Cheating: Gaining Advantage in Videogames*. Massachusetts Institute of Technology, 1985.

[6] Matt deWet and David Straily. Peeking into valorant's netcode, 2020. `https://technology.riotgames.com/news/peeking-valorants-netcode#:~:text=Peeker's\%20advantage\%20is\%20an\%20artifact,opponent\%20on\%20the\%20other\%20side`.

[7] Shawn M. Doherty, Devin Liskey, Christopher M. Via, Christina Frederick, Jason P. Kring, and Dahai Liu. An analysis of expressed cheating behaviors in video games. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 58(1):2393–2396, 2014.

[8] Nisha Ellis. Security and online gaming: Understanding anti-cheat, 2020. `https://hub.schellman.com/blog/security-and-online-gaming-understanding-anti-cheat`.

[9] Jon Espenschied. No security reprieve from blizzard's warden, 2007. `https://www.computerworld.com/article/2545180/no-security-reprieve-from-blizzard-s-warden.html`.

[10] Akshon Esports. Valorant's always on anti-cheat: Vanguard - should you be concerned?, 2020. https://www.youtube.com/watch?v=hDq_EJ5xxKM.

[11] Epic Games, 2022. https://www.easy.ac/en-us/.

[12] Garbaj. Aimbot cheats are evolving, 2022. https://www.youtube.com/watch?v=DlsBaQWfE58.

[13] Blizzard Guides. What its like aimbotting in overwatch 2020, 2020. https://www.youtube.com/watch?v=1oVuSukS5Gk.

[14] hackmag. Deceiving blizzard warden, 2016. https://hackmag.com/uncategorized/deceiving-blizzard-warden/.

[15] Robert Stafford Hardy. Cheating in multiplayer video games, 2009.

[16] BattlEye Innovations, 2022. https://www.battleye.com/.

[17] Jared. Understanding how cheats work, 2009. https://steamcommunity.com/sharedfiles/filedetails/?id=1873537304.

[18] Blame The Controller Overwatch. Overwatch playable talon bosses! - hero select exploit!, 2018. https://www.youtube.com/watch?v=zIHejFrhUQ0.

[19] Jeni Paay, Jesper Kjeldskov, Daniele Internicola, and Mikkel Thomasen. 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, New York, NY, USA, 2018. Association for Computing Machinery.

[20] Jeni Paay, Jesper Kjeldskov, Daniele Internicola, and Mikkel Thomasen. 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, New York, NY, USA, 2018. Association for Computing Machinery.

[21] Qualtrics, 2022. https://www.qualtrics.com/.

[22] Wannes Ribbens, Yorick Poels, and Gertjan Lamotte. Fail with honor or win by cheating: A qualitative and quantitative exploration of cheating. 2013.

[23] Katie Salen and Eric Zimmerman. *Rules of Play: Game Design Fundamentals*. The MIT Press, 2003.

[24] Rashmini Sharma, Gurmeet Singh, and Shavneet Sharma. Competitors' envy, gamers' pride: An exploration of gamers' divergent behavior. *Psychology & Marketing*, 38(6):965–980, 2021.

[25] Irene Serrano Vázquez and Mia Consalvo. Cheating in social network games. *New Media & Society*, 17(6):829–844, 2015.

[26] Li Wang, Liu Fan, and SungMin Bae. How to persuade an online gamer to give up cheating? uniting elaboration likelihood model and signaling theory. *Computers in Human Behavior*, 96:149–162, 2019.

[27] Tyler Wilde. The controversy over riot's vanguard anti-cheat software, explained, 2021. `https://www.pcgamer.com/the-controversy-over-riots-vanguard-anti-cheat-software-explained/`.

[28] Yuehua Wu and Vivian Hsueh Hua Chen. Understanding online game cheating: Unpacking the ethical dimension. *International Journal of Human–Computer Interaction*, 34(8):786–797, 2018.

[29] Xiang Zuo, Clayton Gandy, John Skvoretz, and Adriana Iamnitchi. Bad apples spoil the fun: Quantifying cheating in online gaming, 2016.

Appendix A

Known cheats

This appendix lists several known cheat programs used by cheaters, alongside with the commonly used name for the cheat when such a name exists. Note that even simple types of cheats come in different variations. The 'aimbot' cheat for example has at least five different variations, with each variation working in a different way and serving a slightly different purpose. No details about the variations of the cheats will be mentioned, only what they do in general. For a better understanding and visualization of some of these cheats, we provide a few resources:

- CSGO steam page with GIFs of what cheats look like in-game [17].
- Cheating in Overwatch, including an example of an AI in action [13].
- Cheating in Valorant and discussion of Vanguard anti-cheat safety [10].

A.1 Known cheats

This is a non-exhaustive list of known cheats used by cheaters:

- Aimbot: A program that aims for you so you (almost) never miss a shot.
- Wall-hacks / X-ray: A program that lets you see other objects trough walls, so that you always know where that object is. Usually used to see other players or valuable items.
- B-hop (or bunny-hop): A program that allows you move at ridiculous speeds.
- Fly-hacks: A program that allows you to fly.
- Kill-aura: A program that automatically attacks anything that gets too close.

- "TP-hacks": A program that allows you to teleport to other locations. Usually used to avoid certain death or reach normally unreachable locations on the map.
- Anti-knockback: A program that nullifies any incoming knockback (an effect that causes you to be moved backwards) so you cannot be moved by another player's attack's.
- Invincibility: A program that nullifies any incoming damage so you cannot be killed.
- Invisibility: A program that makes you invisible to your opponents.
- Extra Sensory Perception: A program that reveals information that should not be accessible to you, such as whether a player has a current ability available, how much health they still have or what things they are carrying with them. Sometimes also includes built-in wall-hacks.
- "Reactors": A collection of unnamed programs. Programs in this collection are typically game-dependent but are generally used to perform some action when a certain thing happens. For example: Automatically transferring items when a container is opened, or automatically using some ability A when someone uses an ability B against you.
- AI: A program that uses an AI to literally play the game for you, typically by using many other cheats in combination.
- "Game Asset Access": A cheat that gives the user access to game assets you should not have access to. As an example, some cheaters used this type of cheat in Overwatch to gain access to certain AI enemy models used in events [18]. The AI enemies that this cheat allowed you to control had far more powerful abilities then normal playable characters and also tend to have much more health, making them more difficult to kill than regular player heroes.

Appendix B

Survey Results

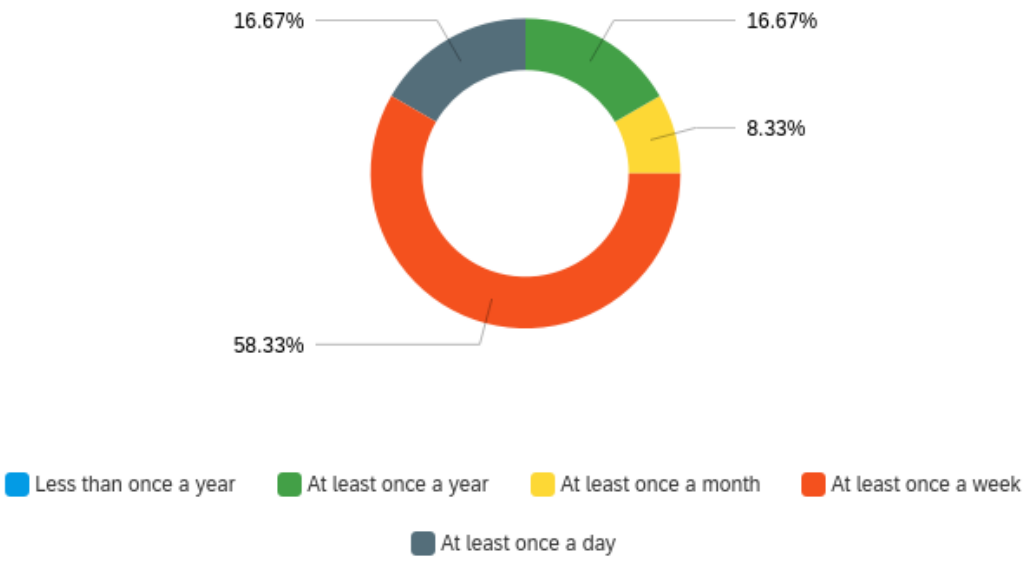

Figure B.1: Frequency of participants playing online multiplayer games

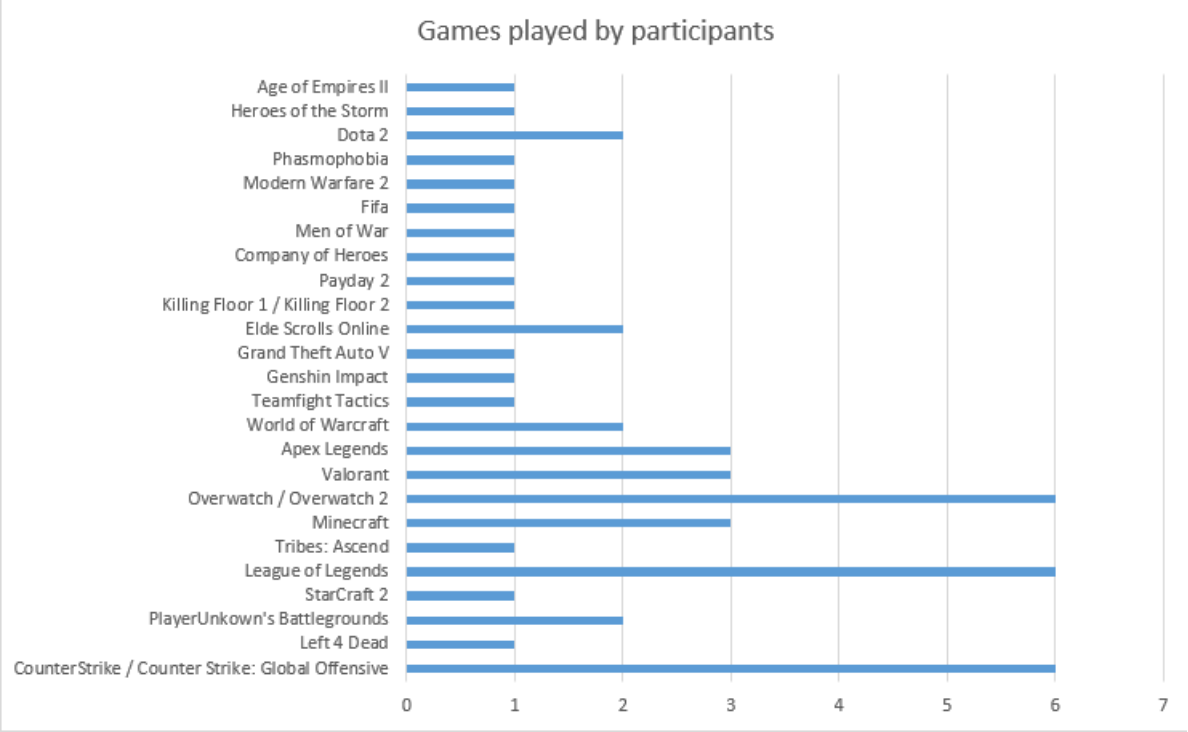

Figure B.2: Games played by participants

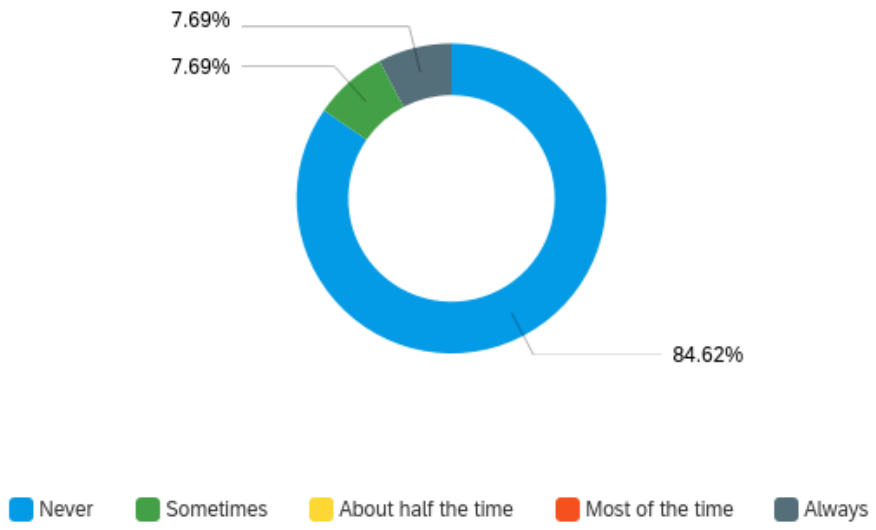

Figure B.3: How often a participant cheats

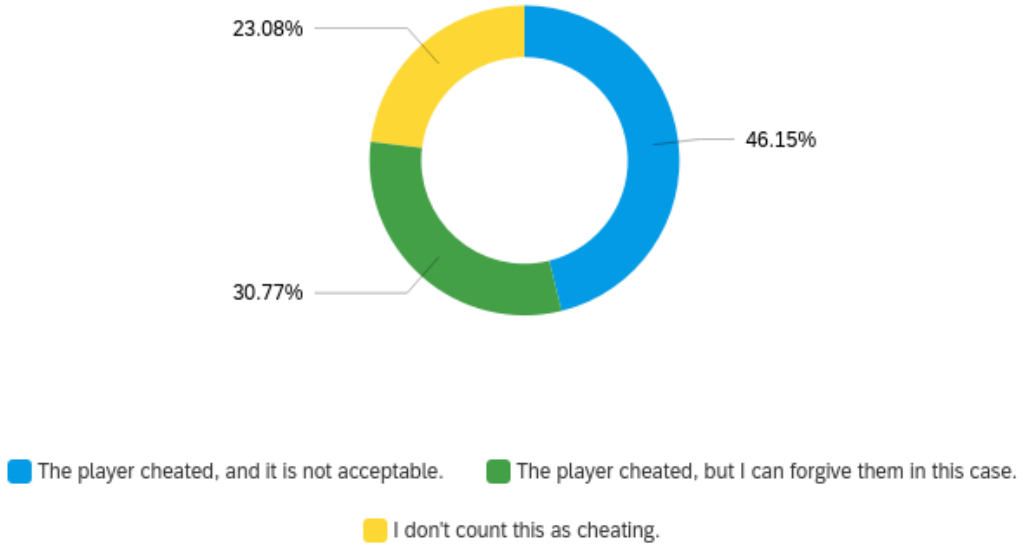

Figure B.4: Scenario 1: Cheater with high ping

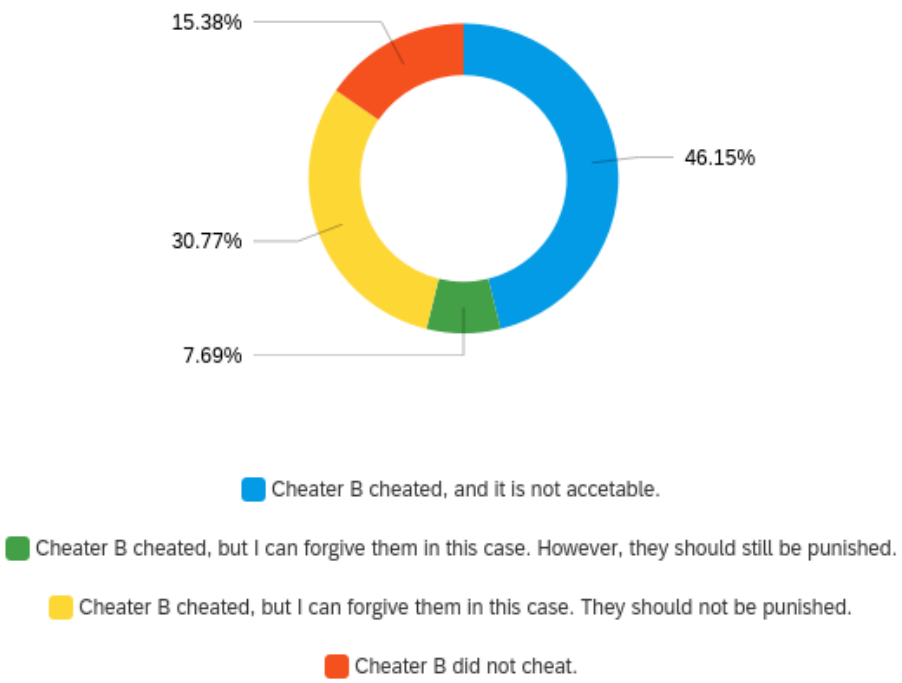

Figure B.5: Scenario 2: Cheater B stops Cheater A from influencing the match

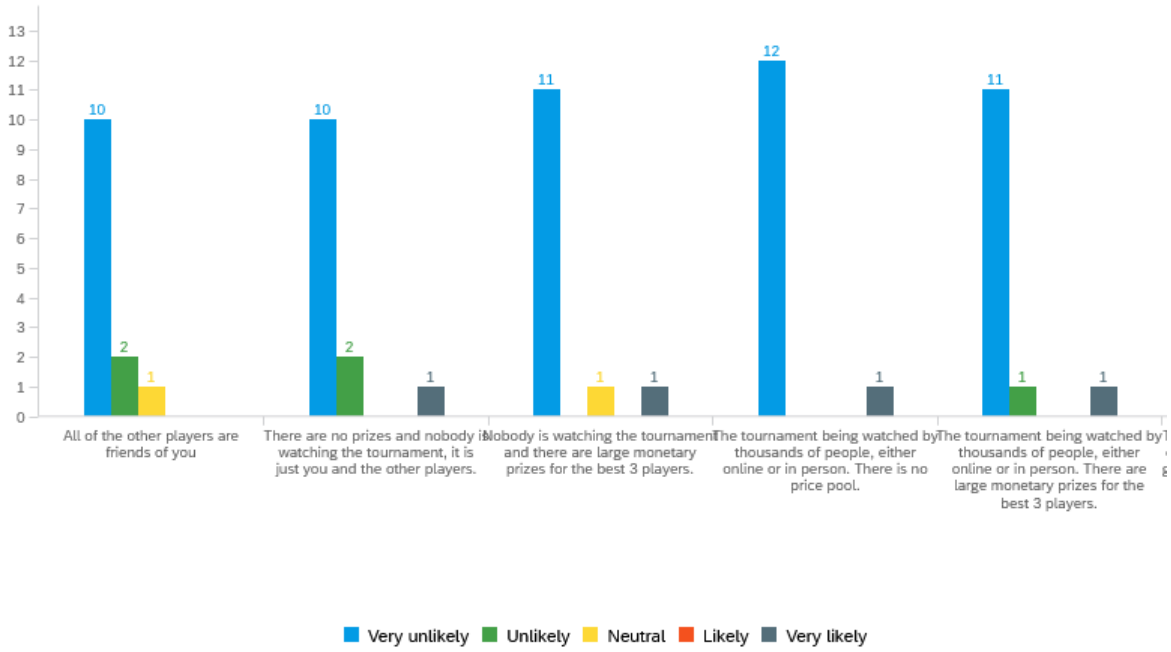

Figure B.6: Scenario 4: Cheating in a tournament (1/2)

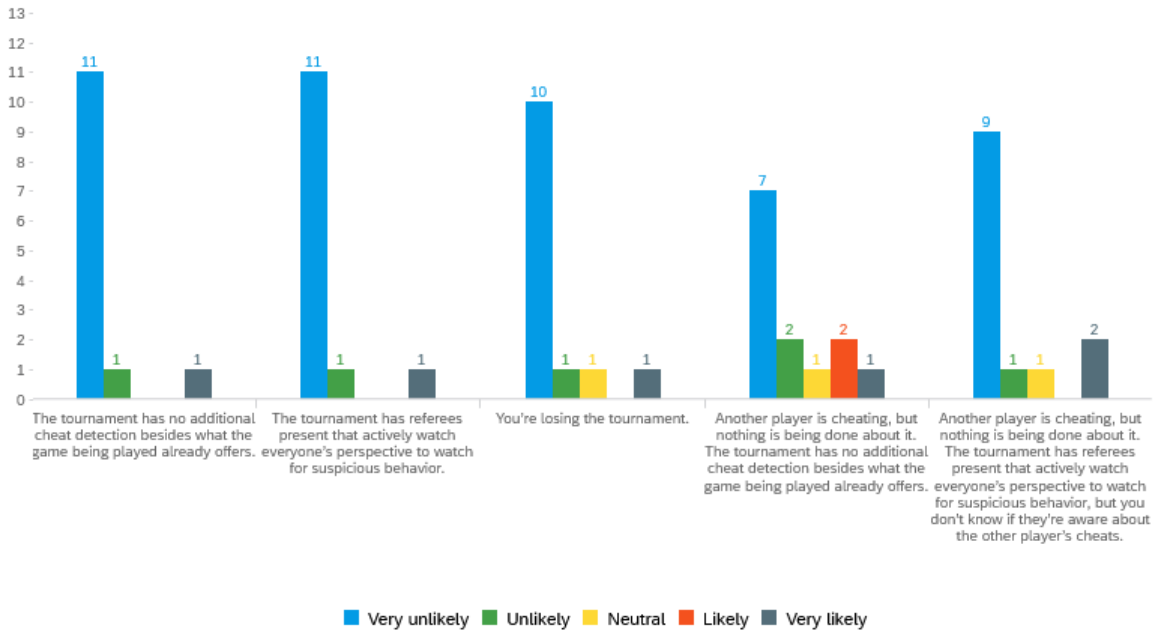

Figure B.7: Scenario 4: Cheating in a tournament (1/b)

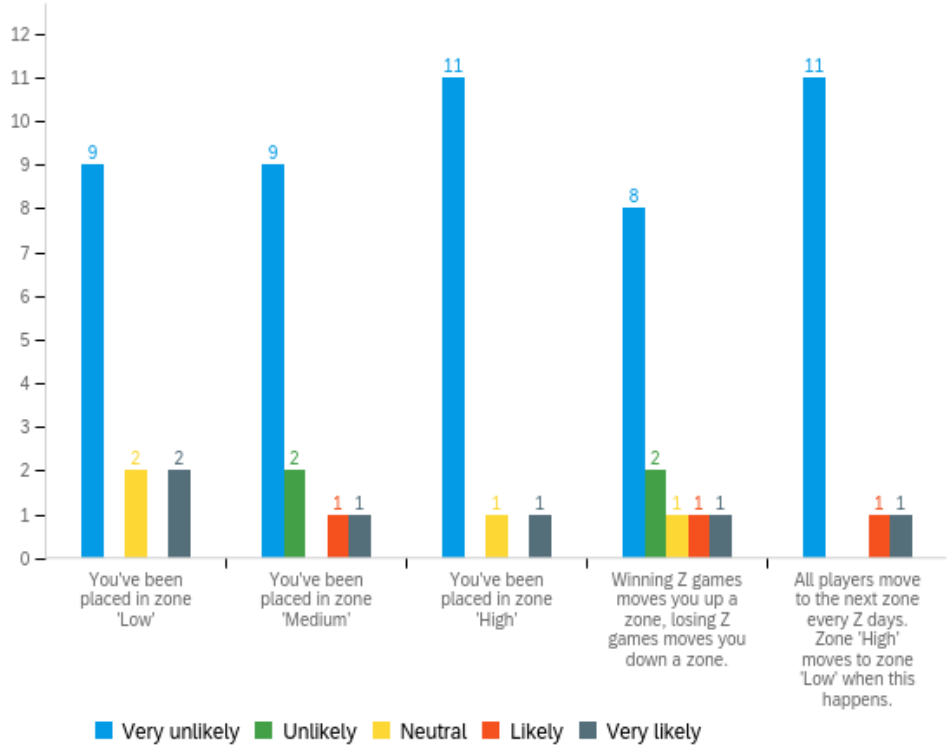

Figure B.8: Scenario 5: Unfair resource spread

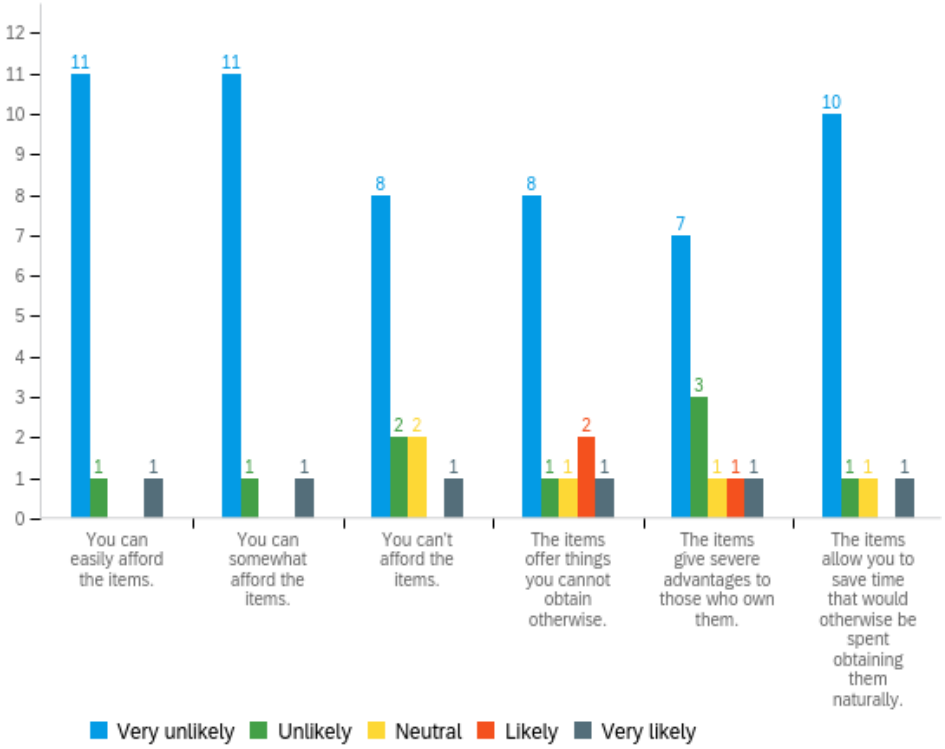

Figure B.9: Scenario 6: Micro-transactions

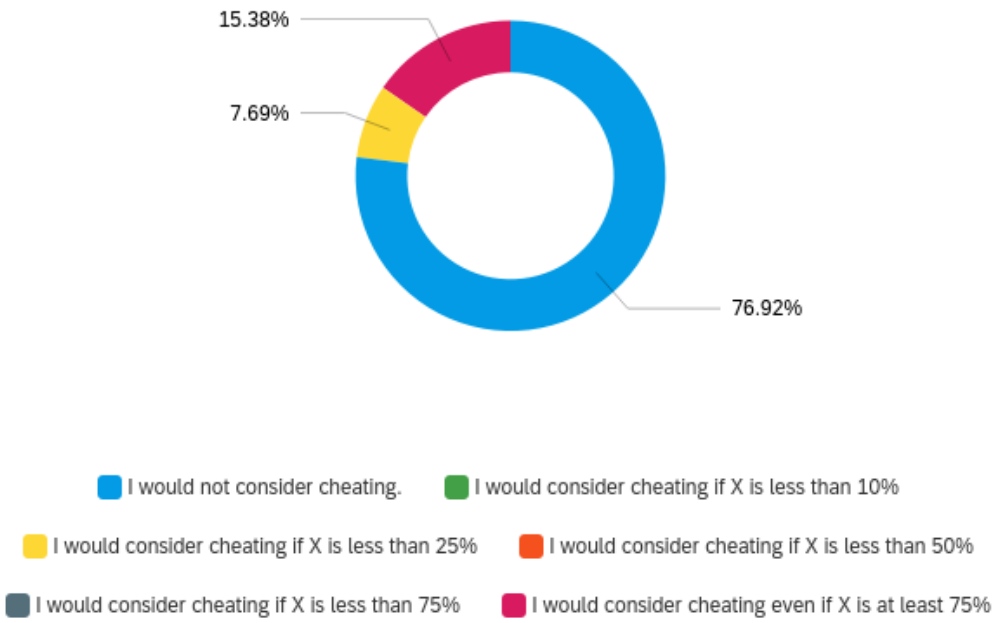

Figure B.10: Scenario 7: X% of cheaters is caught by anti-cheat system

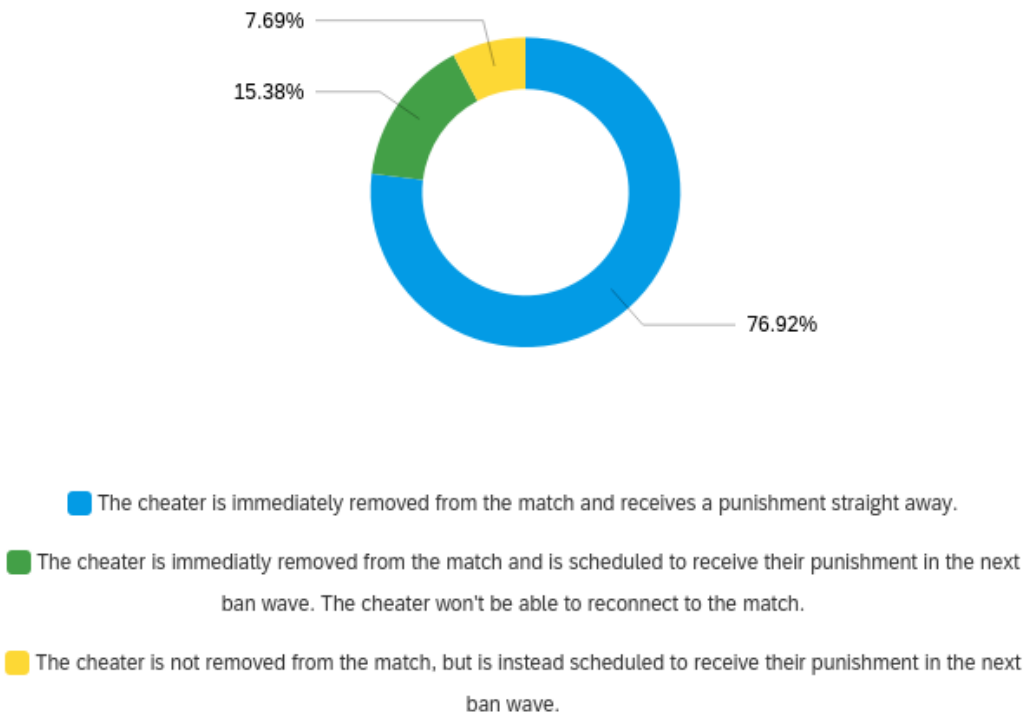

Figure B.11: Scenario 2: What should happen to a caught cheater?

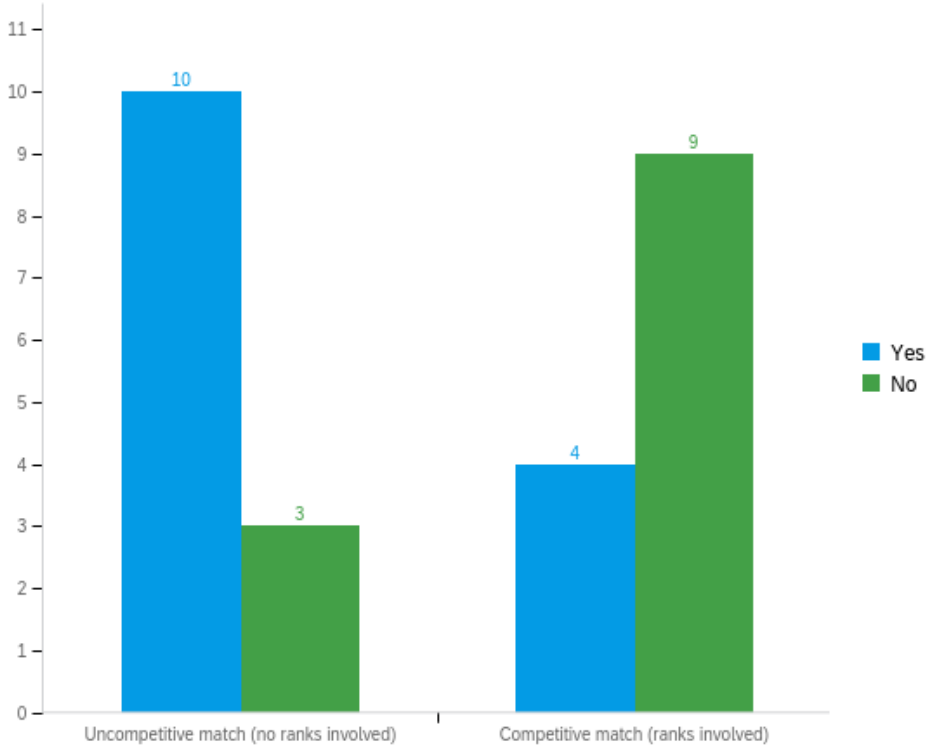

Figure B.12: Scenario 3a: Should a new player be added if one is removed for cheating?

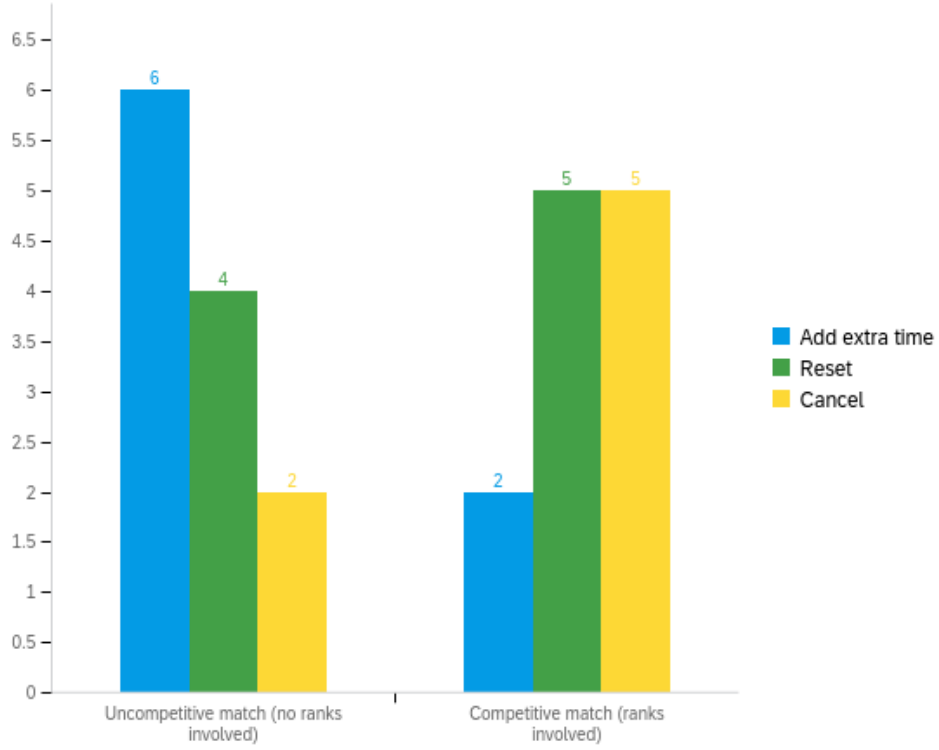

Figure B.13: Scenario 3b: What should happen to the match if a player is removed for cheating?

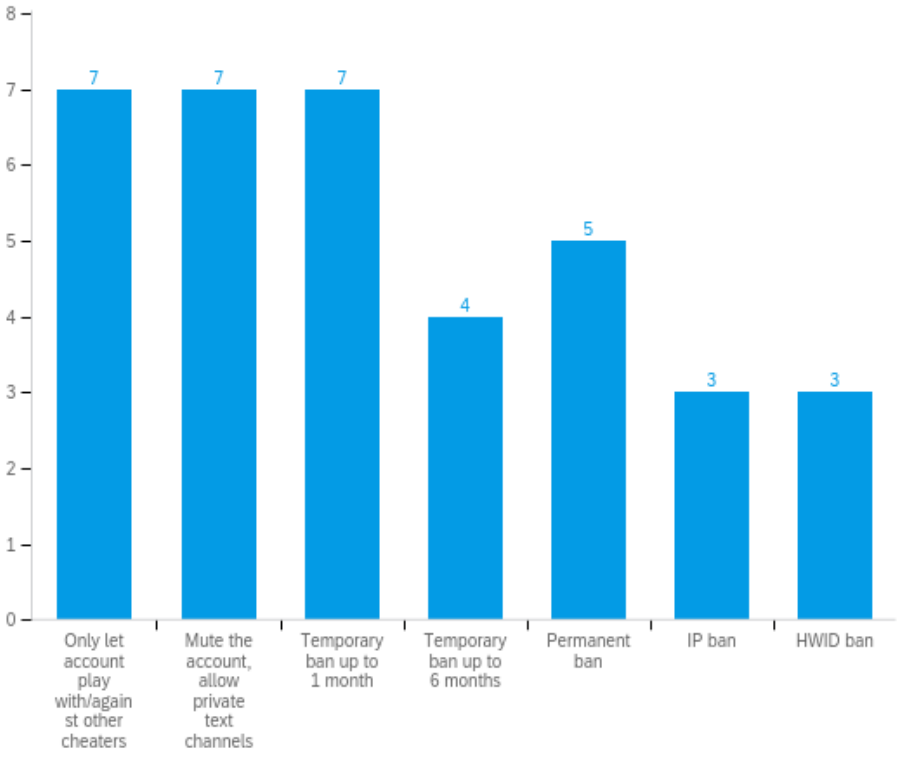

Figure B.14: Scenario 4: What punishments may an anti-cheat system apply?