"Is It Legit, To You?". An Exploration of Players' Perceptions of Cheating in a Multiplayer Video Game: Making Sense of Uncertainty

“Is it Legit, To You?”. An Exploration of Players’ Perceptions of Cheating in a Multiplayer Video Game: Making Sense of Uncertainty

Arianna Boldi[a]* and Amon Rapp[b]

[a] *Department of Psychology, University of Torino, Torino, Italy; ORCID: 0000-0002-2825-3443*

[b] *Computer Science Department, University of Torino, Torino, Italy; ORCID: 0000-0003-3855-9961*

This is an Accepted Manuscript of an article published by Taylor & Francis in International Journal of Human-Computer Interaction on 2023, available online: https://www.tandfonline.com/doi/abs/10.1080/10447318.2023.2204276

To cite this article: Arianna Boldi & Amon Rapp (2023) “Is It Legit, To You?”. An Exploration of Players’ Perceptions of Cheating in a Multiplayer Video Game: Making Sense of Uncertainty, International Journal of Human–Computer Interaction, DOI: 10.1080/10447318.2023.2204276

*Corresponding author: Arianna Boldi

University of Torino, Department of Psychology – Via Verdi 10, 10124 Torino, Italy

Mail: arianna.boldi@unito.it

"*Is it Legit, To You?*". An Exploration of Players' Perceptions of Cheating in a Multiplayer Video Game: Making Sense of Uncertainty

Abstract. Cheating is a major concern for any gaming environment, but effective solutions are still far from being found. Previous research has overlooked the social complexity of current video games and the role that technology may have in determining the cheating practices. In this article, we explore how cheating unfolds within *Call of Duty: Warzone* through a digital ethnography, analyzing the perspectives of both amateur players and video game streamers and how technology shapes the cheating phenomenon. We highlight that players' perception of cheating depends on the "social role" of the cheater. Moreover, the technological sophistication of cheats makes them uncertain in the players' eyes, contributing to the spreading of mutual suspicion and surveillance practices. Based on these findings, we offer a novel understanding of cheating as a sort of black box that only a few individuals are able to decipher, and several design considerations addressing the cheating practices in contemporary games.

Keywords: cheating, video games, First-Person Shooters, FPS, multiplayer, surveillance, sense-making, organizations, psychology, Human-Computer Interaction, HCI

1. Introduction

Cheating is widely acknowledged as one of the most problematic issues affecting online gaming worlds, especially in competitive video games like First-Person Shooters (FPS) (Yu et al., 2012). Technically speaking, cheats are third-party software that crack the original game code to enable gaming actions that would be impossible to perform otherwise, like automatically targeting an enemy (Blackburn et al., 2012). The uncontrolled spread of these unfair practices may reduce the gaming company's profits (Du & Chen, 2009; Chen & Wu, 2015), damage its reputation (Consalvo, 2007) and undermine the players' experience (Irdeto, 2018), who may even decide to abandon the game (Davis, 2002). A great amount of money is therefore spent by the gaming industry to develop anti-cheat software (Kaplan, 2017), but cheat creators are always ready to bypass these technical defenses (Morris, 2003). Cheating is thus an endemic problem of video games, whose eradication through technological means is currently far from being achieved.

Research on cheating could then benefit from an investigation of the human side of the phenomenon, whose understanding may lead to design more effective countermeasures that do not rely exclusively on technology development. Previous research adopting a "human-centered approach" conceptualized cheating as anything that provides an unfair advantage over other players (Botvich et al., 2010): however, different players may attribute the label of "cheating" to different gaming behaviors (Consalvo, 2007; Yan & Choi, 2002), thus showing to be involved in an incessant interpretative activity of what is legitimate and what is not (Consalvo, 2005). Recent human-centered research has focused on the context within which cheating occurs, exploring how players' social relations (Blackburn et al., 2014), cultural in-game values (e.g., Dumitrica, 2011), and the game genre may affect the cheating phenomenon (Witschel & Wressnegger, 2020). Nonetheless, this research underestimates the role of technology, that is how the game software and hardware may shape the cheating practices, as well as does not consider the different "figures" (e.g., players, streamers) that populate the contemporary gaming environments.

In sum, both the "technical" and "human-centered" approaches appear insufficient in

explaining contemporary cheating practices. It is therefore needed to combine these perspectives, looking at cheating as a socio-technical phenomenon that can be better understood by adopting a Human-Computer Interaction (HCI) lens. In fact, technological advancements are making unfair practices more difficult to be recognized and much more "evanescent." As researchers are seeking design solutions that often rely on the players' ability to detect illegitimate players (e.g., Steam, 2021), it is needed to study how players make sense of such an indeterminate phenomenon and the role that technology plays in shaping their perception of cheaters. Moreover, different kinds of social actors may respond differently to the same technology environment: amateur players and streamers play games moved by different motives, understand their gaming practices differently (e.g., as a mere entertainment or as a "work") and thus may react differently to cheating. However, until now we know little about how these different kinds of players may diversely respond to cheating within a certain game.

In this article, we want to investigate the socio-technical aspects of cheating, exploring how players' perceptions of cheating practices are tied to both the different social actors that participate in the gaming social environment (streamers and amateur players) and the technical and design characteristics of the game. To this aim, interesting insights can be drawn from the examination of First-Person Shooter (FPS) games, which are particularly plagued by cheaters (Meades, 2015; Chui et al., 2021). We conducted a 9 month-long digital ethnography within Call of Duty: Warzone collecting a rich amount of data from different sources, like participant observation of in-game activities and semi-structured interviews with players. Warzone has been chosen for its popularity, the richness of its social environment, and the discouraging results it achieved in battling game "criminality" so far. Besides, to the best of our knowledge, there are no previous studies that address cheating in this game. In so doing, we attempted to answer the following research question: How do players perceive and make sense of the cheating practices performed in their gaming environment?

Our contribution to HCI is threefold. First, we provide an in-depth account of the practice of

cheating performed in a gaming community by different social actors. This investigation remarks the contextual nature of cheating, which also depends on the socio-material conditions of players and the "role" played by the cheater. Second, we provide a novel understanding of cheating, highlighting that it is characterized by an intrinsic uncertainty sustained by the technology and the game design features. Third, we present three design implications that may help researchers and practitioners find a solution for the cheating problem, when a completely reliable technological solution is not available.

The article is structured as follows. Section 2 recounts previous research on cheating and outlines the setting of this study, whereas Section 3 describes the method that we used. In Section 4 we report the study findings. Section 5 discusses the findings and outlines a series of implications for design. In Sections 6 and 7, we point out the limitations of the study and conclude the article.

2. Background

2.1 Defining cheating: a multidisciplinary challenge

The concept of cheating in digital games has been described and debated over the last years within a variety of research areas, like game studies, sociology, philosophy, HCI, and computer science, with a marginal contribution from psychology. Hitherto, research on cheating has typically followed two different main approaches, that is *formalist* and *situationist* (Meades, 2015). The first one, which relies on computer science tradition, looks at the formal aspects of games (e.g., the game rules) (Smith, 2006), independently of the context in which people play (Lankoski & Björk, 2015). Hence, formalist studies on cheating are generally aimed at i) elaborating a comprehensive taxonomy of deviant behaviors (Yan & Choi, 2002; Yan & Randell, 2005), or ii) offering technological solutions to manage, prevent and contrast their occurrence (for a review, see Webb & Soh, 2007). The second one, which originates from humanities, is interested in how players attribute meaning to play in a well-defined context (Meades, 2015). This kind of research has explored players' attitudes and beliefs towards cheating (Chen & Ong, 2018; Passmore et al., 2020;

Consalvo, 2005, 2007), as well as possible motivations to cheat (Ribbens et al., 2011; Wu & Chen, 2013).

Within the latter approach, another distinction can be drawn between those researchers who have dug deep into specific cheating behaviors (e.g., Paay et al., 2018; Dumitrica, 2011) and those who provided a more general interpretation of the phenomenon (e.g., Powers, 2003; Morris, 2003; Hamlen & Blumberg, 2015). In particular, much effort has been put in giving an overarching definition of cheating, setting clear boundaries between cheating and a universe of "dark" practices that are different but still deeply intertwined with it, like "metagaming" (Boluk & LeMieux, 2017), "counterplay" (Meades, 2015), "transgressive play" (Aarseth, 2014), "grief-play" (Kücklich, 2009; Parker, 2007), "modding" (Chen & Ong, 2018), and players' exploitation of "bugs" (Bainbridge & Bainbridge, 2007). Despite the theoretical difficulty to differentiate the notion of cheating from these co-related practices, a tentative consensus has been reached on the definition of cheating as a form of "deviant behavior" (Duh & Chen, 2009).

This conceptualization implies two main underlying assumptions. The first one is that using cheats in a game is somehow in contradiction with the idea of playing a game itself. Since games are generally defined by their rules, when these are rejected and disrupted the play-world might fall apart, causing the end of the game and the abandonment of playing (Consalvo, 2007; Huizinga, 1955). In this sense, research focuses on cheaters themselves, with the aim to understand how transgressive behaviors spread within a game world, why some players cheat while others do not (e.g., Wu & Chen, 2013; Sharma et al., 2021) and what their motivations are (Consalvo, 2005; Consalvo, 2007). The second assumption is that cheating occurs in contrast to a common norm which is supposed to regulate the conduct of players, which is generally context-specific: this means that players' behaviors are tied to the rules that are embedded in the game code by the designers (Salen & Zimmerman, 2003) but also to the culture encouraged by the gaming environment and the design of the game (Dumitrica, 2011).

However, what distinguishes a deviant behavior from a "playing style," i.e., idiosyncratic preferences in playing the game that, nonetheless, might result in giving the player an advantage while ruining the fun of other players (such as camping in a shelter instead of facing the enemies in open battle, Yan & Choi, 2002), is not completely clear and even players might find it difficult to differentiate the two phenomena.

In synthesis, an absolute agreement over the definition of cheating appears hard to reach, as this phenomenon overlaps with other phenomena, as well as is strongly circumstantial (Chen & Wu, 2015), since for a behavior to be defined as deviant depends on the context in which it is performed.

2.2 Cheating as a contextual phenomenon

The importance of the "context" where cheating occurs has been pointed out by scholars of different disciplines. In previous research, the "context of cheating" has been mainly understood as i) the *social context*, ii) the *gaming culture*, and iii) the *design features* which may ultimately enable cheating behaviors.

As for the *social context*, researchers have proposed different theoretical models to identify the individual and social variables that drive transgressive players. Drawing upon Bandura's (1989) social-cognitive theory, Wu & Chen (2013) concluded that both the social environment (general peers and significant others) and personal factors (e.g., attitude and valuation of game cheating) determine behavioral differences related to cheating among gamers: for instance, the more often a player witnesses others using game cheats, the more often she would reproduce the cheating behavior (Wu & Chen, 2013). In a similar vein, Sharma et al. (2021) proposed a framework that considers additional variables of cheating behaviors, such as the envy experienced by players towards other players' ranking and their ethical judgment of unfair behaviors. Moreover, gamers' intention to cheat increases if people who are important to them (e.g., online gaming friends, members of the family) perceive cheating as acceptable. Likewise, Blackburn et al. (2014) proposed to look at cheating as a consequence of behavioral contagion, which means that the likelihood of

becoming a cheater increases when the player has cheating friends. Anonymity is also a relevant factor, as playing with strangers online significantly increases cheating practices (Chen & Wu, 2015). Despite the value these studies have in highlighting several social variables relevant for understanding cheating behavior, a variety of questions still remain open, concerning, for instance, why cheating occurs more frequently in certain gaming environments.

Research tackling the *gaming culture* precisely highlights that the definition of what is legitimate and what is not in a video game and the manifestation of unfair or fair behaviors are rooted in players' system of values. Drawing on this assumption, several studies (Dumitrica, 2011; Taylor, 2003; Wright et al., 2002) have extensively analyzed a particular game world to identify how the combination of values, rules and norms may shape the players' behavior, attitudes, and expectations towards cheating. In particular, competitive environments are well-known for influencing unfair behaviors, especially when individuals compete in larger pools (Chui et al., 2021). This finds confirmation also in virtual game worlds, with Meades (2015) highlighting how the "laddish" culture of certain multiplayer games like Call of Duty (COD), which entails a masculine environment that values hostile interactions and communication, may create the condition for the occurrence of dark behaviors. Likewise, Dumitrica (2011) showed that acceptance and normalization of cheating practices by players themselves are profoundly tied to the spread of neo-liberal values (e.g., wealth, success, social status) within the game worlds. This said, both the authors analyzed the emergence of a "culture of cheating" also in view of the games' characteristics. For Meades (2015), the possibility of being measured by other players (e.g., through ranking) while playing is believed to emphasize rivalry and competition, thus exacerbating a culture of hierarchical dominance that encourages cheating. Likewise, the capitalist values that inform the game studied by Dumitrica emerge from its design: for instance, having access to certain items, which are extremely rare to obtain, is crucial to reach in-game objectives, so that resorting to cheating appears inevitable for most players (Dumitrica, 2011).

This brings us to a third line of research, which showed how cheating differently manifests itself depending on the *design features* of the video game: the game mode (single player or multiplayer), the platform on which the video game is played (e.g., console, PC, mobile), and the game genre appear here particularly relevant. The game mode, which differentiates single-player games from multiplayer games (Kücklich, 2008), may consistently affect cheating-related phenomena (see Consalvo, 2007; Meades, 2015; Doherty et al., 2014). When it is performed in a solo situation, players conceive cheating in a more positive light, and are often motivated to cheat by being unable to progress any further in the game (Consalvo, 2007; Kücklich, 2008). Instead, in multiplayer games players cheat to gain an unfair advantage over other players (Consalvo, 2007; Parker, 2007) or to keep up appearances with respect to the community (Doherty et al., 2014), but here cheating may be interpreted as an antisocial activity (Consalvo, 2007). In fact, encountering opponents who make use of hacks is generally a frustrating and negative experience for players (Irdeto, 2018). Moreover, cheating-related practices and meanings are continually being redefined as new gaming platforms appear (Vázquez & Consalvo, 2015). This is well shown by the advent of Social Network Games (SNGs), as players attribute different meanings to cheating when it occurs on Facebook: most SNG players believe that transgressive practices are not necessary, as SNGs are played mainly for relaxation and not for competing or performing (Vázquez & Consalvo, 2015).

As for the game genre, it heavily influences the set of gaming hacks available (Kücklich, 2008; Witschel & Wressnegger, 2020), each one altering the players' experience of the game in specific manners (Kücklich, 2007). As the game genre appears a fundamental factor in shaping the cheating practices, the next subsection extensively recounts previous literature investigating cheating in FPS video games, which is the game genre tackled by the present study.

2.3 The significance of the genre: cheating in Multiplayer Online FPS video games

Two specific game genres have been most frequently addressed in research on cheating: Massively Multiplayer Online Games (MMOGs), which refers to games gathering a huge number of players

interacting simultaneously within the same virtual environment (Webb & Soh, 2007), and FPS, which are shooting video games where players experience combat in a first-person perspective (Voorhees, 2014).

Cheating is a major concern for MMOGs (Mulligan & Patrovsky, 2003), due to the size of their social environments, and the multiple forms that players' interactions may take in there. The same holds true for FPS (Webb & Soh, 2007), since they have been historically suffering from the continuous development of new sophisticated cheating methods (Yu et al., 2012). This is due to the very competitive nature of these games and the fact that they require years of training to be played at best (Yu et al., 2012), which may encourage players to seek easier methods to succeed. Moreover, moral disengagement, and therefore cheating, are argued to be more prevalent in violent video game genres such as FPS, since they reward "immoral" behaviors (Gabbiadini et al., 2014).

Meades (2015) analyzed the so-called *counterplay* activities, which comprise but do not limit to cheating, in different video games of the Call of Duty (COD) franchise, which were released from 2003 to 2014. As we reported previously, Meades showed how these behaviors are deeply rooted in a video game culture, with the consequence that transgressive actions can hardly be eradicated. This results in a continuous battle between developers and game hackers (Morris, 2003), who can always employ techniques for avoiding the detection of anti-cheat software (Feng et al., 2008).

For this, the development of new cheating detection algorithms can be only a part of the strategy to fix cheating (Koskinas, 2018). Yet, the majority of research targeted at cheating in FPS did address the issue merely from the perspective of the technology, whereby most efforts have been devoted to the development of technical measures for both detection and prevention of cheating. This kind of research aims to automatically detect different cheats, such as a) *boosting* (Conroy et al., 2020), a unique form of cheating aimed at rapidly increasing one's competitive ranking; b) *wallhacks* (Park et al., 2020), which enable cheaters to spot an enemy player who is hidden by walls or other occluded objects; c) *aimbots* (Yu et al., 2012), supporting the player in the

acquisition and tracking of targets; d) *game bots* (Chen et al., 2008), automated programs that are used to enhance routines and rapidly get higher scores. Some of these techniques were developed and tested in commercial video games such as *Quake II* (Chen et al., 2008), *Unreal Tournament III* (Galli et al., 2011), and *Counter-Strike: Global Offensive* (CS:GO) (Jonnalagadda et al., 2021).

Although these automated techniques are more and more used (e.g., Galli et al., 2011; Yu et al., 2012), anti-cheating systems may also involve players in the process. For instance, Botvich et al. (2010) have proposed a reputation system based on accusations of cheating made by other players. Player's spontaneous report is considered a successful method to block cheating, but can lead to mistaken conclusions (Jonnalagadda et al., 2021), since players might not correctly recognize and report a cheating behavior. In 2019, CS:GO started using Steam Trust, a surveillance system which is based on the presence of Overwatch Investigators who are required to "*review reports of disruptive behaviors, determine whether those reports are valid, and apply bans if appropriate*" (Steam, 2021). These investigators are selected on the basis of their knowledge of the game, which might help them make more accurate judgments about gaming behaviors. While the idea is interesting, there are no current studies concerning, for instance, what skills players need or what criteria they employ to arrive at a precise verdict. In fact, it is not clear on what basis do players assess the "culpability" or not of their opponents, how much their perception is accurate, and by what factors it might be influenced.

In sum, cheating appears as a complex phenomenon that both players and game developers cannot fully control or prevent. It seems that mere technological means cannot be a definitive solution for the problem, as cheating may be rooted in the values and meanings that players ascribe to their own and others' in-game behaviors. By contrast, only relying on players' reporting may incur in biases and mistakes, which may depend on the players' expertise and even their "role" in the community. In this complex landscape several aspects of cheating as a "human phenomenon" are still unexplored by previous research.

First, the whole social gaming environment, which is composed not only of "amateur" players but also of online content creators and live streamers, has been poorly investigated with reference to cheating. It is not clear whether different kinds of "gaming actors" may understand and perceive cheating differently and how this may impact on the gaming experience. Such a neglect may be relevant, insofar this complex ecosystem has been becoming more and more pervasive in the digital game culture (Pellicone & Ahn, 2017).

Second, the sophistication of current hacking technology may veil the presence of a cheater within a game environment (Jonnalagadda et al., 2021), making current cheating behaviors extremely ambiguous and evanescent. Research, however, did not investigate how such ambiguity enabled by technology may impact on the players' experience and how cheating is "constructed" by the perceptions and beliefs of the gaming actors, which in turn are affected by "design." Rather, it took for granted the idea that cheating is a "real phenomenon" that can always be identified by players. A thorough investigation of how technology and the design features of a game may influence cheating phenomena is still lacking in current research.

To explore these aspects, which may provide a more complex and multifaceted picture of cheating, we conducted an ethnography in an FPS video game, namely *Call of Duty: Warzone*. Being an FPS that adopts an MMO-style approach, due to the high number of individuals playing in the same virtual environment, this game well represents the game genres that are most affected by cheating. Moreover, it entails a highly competitive interaction among players thus potentially favoring cheating behaviors. The next sub-section describes the key elements of the game explicating their relevance for the topic under investigation.

2.4 Warzone's gaming world: game aspects relevant to cheating

"Call of Duty: Warzone" (a.k.a., "COD: Warzone" or simply "Warzone") is a Multiplayer Online Battle Royale game recently (2020) published by Activision as a *free-to-play* game, i.e., it does not require any payment to be played.

Being a Battle Royale (BR), a sub-genre of shooting games (Ohno, 2021), Warzone blends elements of combat, survival and collection of resources. The matches can be played alone or in teams, composed of two, three or four members: members of the same team fight enemies organized in teams of the same size. Players must kill all the enemy players in the arena to win the game, while a mortal gas cloud progressively shrinks the playable area, thus forcing a more frenetic and dynamic fight. A BR is even more "punishing" and competitive than the classic multiplayer games that have been analyzed in the literature so far: players playing BR can be respawned in the game only thanks to a consistent effort from the squad, which can bring the player back by spending money at a Buy Station. Here, cheating may become extremely relevant: in fact, being killed entails the player's exclusion from the match with the only possibility to observe the teammates while playing, whereas using cheats could ensure permanence in the game world and, eventually, victory.

Another game feature relevant to cheating concerns statistics recording (Meades, 2015). In Warzone, players' performances are constantly monitored and made visible to both fellow players and enemies in the form of numbers. Statistics display detailed information about the player, like the *level*, which relates to the number of points gathered during the gaming sessions, and the *Kill-Death ratio* (K/D), a rapport between the amount of kills executed and the deaths taken. Statistics are believed to influence the way players are assigned to a game session, during which they enter a *lobby*, i.e., a staging area in which players can warm up by fighting against their enemies for about 60 seconds[1]. Cheaters may then manipulate their statistics in order to join lobbies populated by less skilled players or, conversely, to join elite game groups or tournaments with money prizes whose access is limited to players having a certain K/D.

Finally, the social landscape of players in the community of Warzone is quite complex, since the game counted 100-million players in April 2021 and has gained a great popularity also in the social media context, among streamers and followers, counting 750,000 live viewers in April

[1] The term lobby also identifies all the players that participate in a single game session (i.e., the player's team and all the enemy teams).

2021 (Pekmic, 2021). Here, different figures contribute to creating the gaming culture and may impact on the unfolding of cheating (Dumitrica, 2011; Meades, 2015). The great part of Warzone players is composed of "amateur players", who do not receive money from playing but may occasionally participate in non-professional tournaments. They may play the game alone or in a squad composed of random players, i.e., randomly assigned by the system to a team, which is then disrupted at the end of the match. Alternatively, they can join a Regiment, i.e., a clan system that groups people who want to play together in a more continuative way. Differently from amateur players, "streamers" are exposed to an audience and are interested in making profit from gaming and nurture the game fandom with a variety of contents. These incomes mainly come from their activity on social media (e.g., players' subscriptions and advertising). Some of them might also be i) former COD professional players or E-sports players of other video games, ii) players endorsed by Esports organizations and team (e.g., FNATIC, FaZe), or iii) participants to professional tournaments: these players may gain money from winning monetary prizes or earning a regular wage from an E-sports organization. All these players have different motives for playing but interact within the same large game world: in the same lobby, people who play "for fun" (i.e., playing only for enjoyment and to stay together) may have to defeat opponents who play for entertaining their audience or training their skills. Being cheating influenced by social aspects, these complex interactions between different social actors may have an impact on cheating behaviors.

In sum, all these game features make Warzone an emblematic case to study cheating, whereby no previous studies explored the phenomenon in this game. We thus investigated how self-declared "fair" players "construct meanings" around cheating through an ethnography, situating the phenomenon in both its social and technical dimensions, i.e., the entire social environment in which players are immersed, as well as the specific design features characterizing the game.

3. Materials and methods

We adopted a *reflexive* ethnography approach, in which the researcher's experience is considered worthy to be explored on a par with that of the other participants. This perspective has been employed in previous works to study video games (e.g., Rapp, 2018a, 2020). Differently from the realist approach, which seeks to ensure the "objectivity" of the ethnographic recount, reflexivity values the ethnographer's subjective point of view (Van Maanen, 2011), also constantly making her decisions accountable (Cardano, 2009; Rode, 2011; Van Maanen, 2011; Rapp, 2021). Moreover, the reflexive perspective was paired with an auto-ethnographic work (Tedlock, 1991), which is common in digital gaming ethnographies (e.g., Rapp, 2018b): therefore, the ethnographer's personal experiences in *COD: Warzone* became an important part of the data set collected during the fieldwork.

3.1 The ethnographic experience

The ethnographic work was conducted by the first author (from now "the ethnographer") within the Italian community of *COD: Warzone*, from May 2021 to January 2022. Within this period, the ethnographer alternated phases of participant observation and data analysis. She joined the "online spaces" where players of the Italian COD community usually meet and discuss about the game, investigating i) social networks, i.e., players' private groups on Facebook, as well as Instagram pages of streamers, content creators, and tournament organizations; ii) content communities, i.e., Twitch and Youtube channels; iii) social media, i.e., servers on Discord, public groups on Telegram and private WhatsApp groups; iv) and official websites containing guides and detailed descriptions of the battle arena (e.g., callofduty.com).

Moreover, she played the game as a participant observer, participating in 190 matches, for a total of 98 hours, 16 minutes, and 48 seconds of play, and reaching the level 382. During the

[2] These and other data were retrieved through the website https://cod.tracker.gg/warzone, which registers log data and provides statistics about the player and her friends.

ethnographic work she joined a regiment, also entering its private WhatsApp group, counting 128 members. The ethnographer had then the opportunity to play regularly with different players, observe social and organizational dynamics, take part in players' discussions daily, and develop social bonds. In so doing, the ethnographer also focused on the design elements of the game, trying to understand how these may affect the players' individual, social, and organizational behaviors.

3.2 Data collection

The ethnography relies on different data sources whose details are presented in Table 1, namely: ii) participant and non-participant observations of gaming sessions, ii) data coming from social networks and social media like posts, comments and videos, iii) informal conversations, iv) semi-structured interviews, and v) a personal diary.

TABLE 1. HERE

3.3 Sample characteristics

Participants were recruited following two strategies. The first one addressed the players of the regiment in which the ethnographer was involved (N=19). The heterogeneity of this group of participants was guaranteed by the fact that they had different levels of seniority within the group and used to spend time playing both with members of the group and with their personal fellow gamers (e.g., real-life friends, players who were not interested in taking part in a structured group, etc.). Interviewing participants who were already part of the regiment of the ethnographer ensured trust between the researcher and the interviewee, contributing to the quality of the collected data. As a second method of recruitment, the ethnographer adopted a snowball sampling technique, i.e., asking participants to forward a recruitment message, describing the purpose of the study to their fellow gamers. Following a data saturation criterion (Bowen, 2008), the ethnographer settled for 25 participants when she realized that additional data would not have produced new relevant findings.

The sample selection followed a purposeful sampling technique (Marshall, 1996): the sample was differentiated mainly along the dimensions of "competence", i.e., the capability to use skills and knowledge of the game as a resource to reach in-game objectives, which emerged as central in the Warzone community affecting most of the social interactions among players (for instance, how players choose their teammates or the members of their regiment). Assuming that players with different levels of expertise might conceptualize the cheating practices in different ways, we classified participants along their level of competence. To identify the relevant factors affecting the competence of a player, the ethnographer asked four of the most expert players of her regiment what criteria they used to assess the other players' competence to make in-game decisions. On the basis of their suggestions, we identified two relevant dimensions for evaluating the players' competence in Warzone: i) the *experience*, which is defined by the time passed in the game and the number of matches played, and ii) the *ability*, which is indicated by the overall K/D ratio, the number of kills, deaths, and the overall score.

We then recruited 25 participants balancing the sample composition along the two identified dimensions. The recruited participants, who were all amateur players, can then be classified according to the average value of their K/D ratio, the hours spent in the game and the matches played. This results in three main categories, whose characteristics are illustrated in Table 2: i) four *masters* players, ii) eleven *average* players, and iii) ten *novices*.

TABLE 2. HERE

Almost all the participants (N=21) were passionate about video games, having spent 10 years or more playing video games and having had previous experience with other FPS. Ten participants had already tried other games entailing a Battle Royale mode. With the exception of two participants, all the players were members of a regiment, having different organizational roles

(e.g., founders, officers, or soldiers). The average age was 31.64 years (min age = 22; max age = 52; females = 4). Table 3 synthesizes the characteristics of the participants interviewed.

It is worth to notice that the findings reported in the following Sections are grounded in the interviewees' reports as well in all the documents analyzed, social media explored, observations conducted, and casual conversations carried out during the whole duration of the ethnography.

TABLE 3. HERE

3.4 Data analysis

The ethnographer's diary constituted a preliminary level of analysis of the collected data: here, the ethnographer daily summarized the relevant information that she gathered from different sources and reported her personal reflections and insights emerging from their examination. Following Geertz's methodology (1973), at the beginning of the ethnography the field notes were drafted in a more descriptive manner, including a great number of details. As the fieldwork continued, the diary was enriched with more abstract reflections, since the ethnographer started identifying patterns across the observations she made and the data sources she analyzed, elaborated tentative hypotheses emerging from the preliminary analysis, and identified new aspects that were worthy of being explored. Then, the ethnographer informally discussed her hypotheses with the members of her regiment, double-checking her personal interpretations of the collected data and discarding those that did not fit the participants' understanding of the phenomenon.

In addition to that, the interviews and all the relevant quotations reported in the field notes eventually underwent a thematic analysis (Braun & Clark, 2012; Saldaña, 2021), which is a widely used method in HCI for its flexibility and independence of theory and epistemology: an inductive, rather than a hypothetical-deductive stance (Patton, 1990), was then adopted for the whole process.

The analysis was mostly conducted by the ethnographer through the application of open, axial, and selective coding techniques (Strauss & Corbin, 1990). First, she generated 110 initial open codes, by identifying data characteristics that were considered relevant to cheating. Data were broken down labeling sentences with a corresponding code. In a second phase, she grouped the codes into 14 axial categories (e.g., "Cheating technologies", "Source of knowledge", "Values of the community", and so on). Finally, she identified three recurrent themes across the data, which represent the selective codes: the subjective perception of cheating, the mediating role of competence, and the effects of cheating. In addition to that, for the whole duration of the data analysis and even during the writing phase, the ethnographer employed a "participant researcher" strategy (LeCompte & Goetz, 1982), which consists in seeking the aid of the informants to confirm or adjust the interpretation of data. The ethnographer informally asked other members of her regiment questions about her data interpretations and involved a restricted group of four individuals to assess her understanding more in depth.

To protect the privacy of participants and players who published content and/or comments on the Internet, all the players' names and game nicknames will be anonymized in the presentation of the findings. The research has been approved by the ethical committee of the authors' university.

4. Findings

The findings are presented along three main themes. First, we describe how cheating unfolds in Warzone, which characteristics cheats have, and how the phenomenon is perceived by the players. Then, we highlight the importance of "competence" in providing the means to identify cheating behaviors. Finally, we focus on the effects that cheating has on the virtual world considered at large, showing the emergence of a culture of "surveillance," which affects both amateur players and streamers. Table 4 provides a snapshot of the findings.

TABLE 4. HERE

4.1 Cheating in Warzone from the participants' point of view

The analysis of the collected informal conversations, interviews and online content contributed the most to the elaboration of this first theme, which focuses on the players' perception of cheaters and their understanding of the cheating technologies and practices. During the analysis, we paid attention to how players defined and conceptualized cheating behaviors and the characteristics and motives that they ascribed to cheaters. In so doing, we discovered that their understanding of the phenomenon depends on the knowledge they have of gaming technology. Moreover, their perception of cheaters is connected with their socio-material conditions, as well as the cheater's social role (streamer or amateur player) and supposed abilities.

4.1.1 Who the cheaters are

A certain vagueness characterizes the cheating practices in Warzone, starting from the ways players conceptualize cheaters. Cheaters are interpreted by players as dishonest people with scarce sense of morality, who are willing to do whatever it takes to win the game: on the one side, they may spend a considerable amount of money, being cheats (also known as *hacks* in the game community) illegal software available only for purchase; on the other hand, they may take consistent risks, insofar the game company sanctions the cheaters by *banning* their account.

What is interesting to notice here is how players account for cheaters' actions. Cheaters are generally believed to be driven more by the egoistic need to win rather than by the intention to purposefully ruin the others' gaming experience: they are miles away from borderline figures like *trolls*, who are perceived as having a malicious intent to provoke or attack another user in an online environment (Ortiz, 2020). In the participants' recounts, cheaters are mostly seen as "natural born cheaters," because their in-game actions are just a reflection of their personality. Their cheating behaviors are believed to be reiterated in several spheres of their life and be part of their identity: "*it's like the world of drugs, because if you get close to it you end up in another category... it's not like when I used them in single-player games, and I alternated between times when I used the cheat*

codes and times when I did not… I could choose... here it's different, it seems that if you are a cheater in Warzone, that is your identity, you are part of that category of people" (P17). This idea resonates even among streamers, one of which (having 25.959 followers on Twitch) says: "*once cheater, forever cheater*."

Even though participants agree on this overarching interpretation of cheating, by examining the various conceptualizations and definitions of cheaters provided by players, more nuanced perspectives seem to emerge. By and large, there are four kinds of "prototypical cheaters" reported by the participants: a *doper*, a *fraudster*, a *frustrated*, and a *slacker*.

Several participants associated cheating with dark behaviors performed in the sports world, seeing it as a body-free parallel of doping[3] (Yan & Randell, 2005; Laurens et al., 2007). For them, similarly to athletes who take drugs, cheaters should be excluded from tournaments and every game competition. The label of *doper* is especially used with reference to streamers who compete in official matches, like E-sports tournaments, substituting pivotal gaming skills with software used as a performance enhancer (Chanda et al., 2021; Holden et al., 2017). A person who uses game hacks may also be perceived as a *fraudster*, a thief, or a scammer, belonging to the realm of crime (and thus deserving a punishment): the fair penalty for these people is to be excluded from the game world. This group of appellations was particularly directed towards the streamers broadcasting live their gaming sessions, whereby the bond between the streamer and her followers appears to be built on trust.

Instead, the cheater as a *frustrated* person is ascribed with attributes pertaining to the emotional domain, being one who has scarce self-esteem and is incapable of coping with the unsatisfactory feelings emerging from her game experience and personal life: "*people are already frustrated due to the Covid situation… people are not happy… so they look for any gratification… to me it all starts from this, from dissatisfaction and frustration with life in general*," as P11 says.

[3] Doping may be defined as the enhancement of skills via the assumption of substances that are prohibited by the World Anti-Doping Agency and by the law.

Finally, the cheater as a *slacker* is a player who does not have the right skills to play but, at the same time, does not want to make efforts to develop them. They are foreign bodies embedded in the game world, which is based on completely different values, like constant training, commitment, and team spirit. In both these latter cases, cheaters are simple amateur players with no abilities who, nonetheless, are perceived as "parasites" or viruses that may even "infect" other fair players.

However, participants appear to be more benevolent towards those amateur players who cheat but hold abilities resulting from practice and time spent within the game. This kind of players may represent an exception to the four kinds of "negative cheaters" we identified above: "*you may be so annoyed with the game to get to that point* [of buying game hacks]*... it is okay to have a little fun, just don't do it forever"* (P10); while P7 highlights: "*People are sick and tired of finding cheaters at the end of the game, so they buy them too, just to have some fun*." Several participants declared that they play the game merely for fun (e.g., P12) and to escape difficult life moments, like those engendered by the COVID-19 pandemic. In this perspective, using cheats could be a way to have a more satisfying game experience when the battle becomes too hard, offering relief from the difficulties of the real life: participants may understand these cheaters' reasons to cheat, provided that they own in-game abilities and are not streamers, who, instead, must not perform any cheating behavior.

In sum, while cheaters are generally conceptualized in a "negative" way, there are nuances in how they are perceived, which may also depend on the role of the deceiver: a streamer who cheats is more often characterized as a doper or a fraudster due to the public commitment that she has towards her audience, while a novice may be seen as a slacker, as she does not have the abilities to face the game.

4.1.2 What cheats are in participants' eyes

Among all the possible interpretations that players make of cheating extracted from the analyses of the collected interviews, informal conversations, and content posted online, there is a core

understanding on which all the players agree: cheating consists in buying illegal third-party software to purposefully augment the abilities and chances to win the game. That said, there is no absolute consensus on a gray area of in-game behaviors, which may be perceived as cheating or not depending on the participants' beliefs. For instance, several participants include the intentional exploitation of game glitches or bugs into the category of cheating behaviors. Players can temporarily have an advantage by exploiting a glitch – e.g., being invisible, or resistant to the mortal gas cloud – without incurring the cheat costs and risks. As P17 explained, "*for a three-month period there has been this glitch, called the stim glitch… basically you just had to repeatedly use the shot of adrenaline to become immortal to gas… so you could easily hide in the noxious gas area, ride out firefights with enemies, and win the game.*" According to some participants, these kinds of glitches are completely unfair because they destroy the core idea of the game, that is to fight for survival. By contrast, other participants believe that taking advantage of flaws in the game's code should not be considered cheating because "*it's a game error, it's Activision's responsibility*" (P4), suggesting that cheating has something to do with the intentional alteration of code.

Several participants also suggested that there might be other ways to gain advantages, that is, by spending money. This conceptualization of cheats is intrinsically related to the key role played by technology in influencing the outcome of crucial game actions, like killing opponents and escaping death. For instance, the quality of the Internet connection, namely the bandwidth and the latency/ping which may cause delay in the information exchanged with the host, is considered of paramount importance for playing: a bad connection may cause phenomena like *stuttering* – which makes the character appear to skip ahead or freeze while moving, or *hit marker delays* – when the shots landed on an enemy are not effective, which all negatively alter the interaction with the game world to the point of making the match "unplayable." In this sense, for several participants exploiting technological advantages that can be legally bought on the market is still unfair, like the employment of Virtual Private Networks (VPNs), which are generally used to increase the security

of networks. Using a VPN is believed to bring two benefits: it may reduce the "ping," allowing for faster input and better reaction, which are pivotal for a fast-paced game; it allows players to reach foreign servers in different areas of the world, for example, Jamaica, Saudi Arabia, Pakistan, which are considered less performing in terms of Internet connectivity, and in which gamers may thus be easier to defeat.

Some players also believe that spending money on hardware equipment can be considered a subtle form of gaining advantages over the others, as a player explains: "*Having a connection of 1000 Mb, a modified joystick, a 144Hz monitor, a more powerful PC or console … all these things yield considerable advantages, for equal skills, so it is still tricky. If you do the math, an overt cheater spends only, say, 100 euros… the 'moralist' cheater spends way more. Both of them win or can win in an easier way*." Other participants also considered as cheating buying third-party devices like Cronus Max and Cronus Zen, which allow players to digitally modify their controllers to obtain advantages that are not as explicit and obvious as other cheats.

In sum, players agree that cheats are third-party software developed to provide unfair advantages. Nevertheless, certain players define as "cheating" also the utilization of expensive equipment that enhances gaming performance, albeit they are perfectly legitimate in other players' eyes. This is not surprising if we consider that, in Warzone, technology conveys a social status contributing to creating power asymmetries within the game community. Players in Warzone are not equal because they can allocate different resources to the game, which depend on their socio-material conditions (e.g., having enough money to be invested in hardware components). Therefore, in certain players' eyes, who may not have the same resources of other "technology enhanced" players, this leads to an asymmetry that is not balanced "by design," since there is no mechanism in the game that may counterbalance these disparities. For these players, using "classic" cheats (i.e., software specially developed to cheat) may be the answer to this socio-material unbalance, the attempt to counteract the "cheating" of those who have major economical means, subverting a

world that shows the same rules that are enforced in the neoliberal capitalism: harsh competition, struggle to perform, and consumerism.

4.1.3 What participants know about cheating technology

Not only is cheating not univocally defined, but also the knowledge and experience that players have of it vary widely, contributing to making the phenomenon more evanescent.

Some participants were capable of naming certain game hacks and defining their function, yet others were far more approximative in describing existing cheats. By and large, *wallhack*, *aimbot*, and *aimlock* were the most commonly mentioned cheats by the participants: these cheats act on the most important abilities required in FPS games, like spotting the enemy, targeting the most vulnerable parts of the enemy's body, and firing without losing the aim, enabling players to see through any type of obstruction, or assisting them with automatic targeting systems. Other less common cheats emerged in other participants' recounts were flying, becoming invisible or capable of long-lasting running, and suffering no harm when attacked. However, these participants showed that they were not completely sure of these cheats' names, functioning, and, sometimes, even of their actual existence.

The uncertainty concerning cheating is also underpinned by technology. Cheats available for the game are extremely complex and difficult to be recognized even for an experienced eye. Evidence of this can also be found in the discussions carried out on game-related forums, as well as in the videos of streamers who recorded themselves while playing with the aid of cheats[4]. For instance, a cheat like *aimbot* can be customized by adjusting about 20 parameters, and players may set its level of "intensity," which makes its detection difficult when used by an experienced player: "*for instance there is a 'soft-aim', which aims at the body instead of aiming at the head of the enemy, which would make the cheat evident… and then you look at the kill cam thinking ok, this*

[4] Live streams are realized by capturing the screen displaying the perspective of the player's avatar: then, as the streamer controls the functioning of cheats during different moments of the game, the hacking application is visible to spectators.

player is good ... these are cheats but you cannot tell the difference, so you think that there is just a good player in the enemy team" (P16).

4.1.4 Building knowledge around cheating

More than half of the interviewed participants reported that cheating is rampant in Warzone. When encouraged to elaborate on their answer, however, many of them declared that this belief did not originate from their direct experience, as encountering a cheater is a rare event. Players mostly learn about cheats from discussions with seasoned fellow players, from content and "rumors" found on the Internet, or in videos explaining how to deal with the problem. Examples are offered by P1, who says: "*I think I only know one cheat… I didn't understand how it worked, so I got curious, and I really looked for it... (...) it's named 'aimbot' I think... then I also knew other cheats, I have discovered them in videos…*"; or by P15 who highlights the role of the streamers in giving advice "*I talk to streamers while they do their gaming sessions... and sometimes they also answer my questions*" (P15).

As the primary source of knowledge about cheats is indirect, players' acquaintance of cheating appears often partial and imprecise, even because grasping information without becoming a cheater is extremely difficult: "*Then there is this cheat known as 'flymode', but I have only seen it in a video, so maybe it doesn't exist…*" (P10); "*Knowledge about cheats is based on word-of-mouth, there is not much information beyond that… If you try to ask those who create them, they block you*" (P10). Moreover, players are not always able to distinguish a cheat from a technological issue. For instance, *rubber banding*, a consequence of latency, makes the character that is moving in a certain direction jump back to a precedent position, as if it were "teleported." This effect might be mistaken for a cheat: "*Now there is also the speed glitch, and it seems a lag problem of the game... and there was this player who was walking and suddenly he was behind me, and he finally executed me ... but I wasn't sure of what was happening"* (P16).

On the one hand, cheats can be manipulated and customized so as to be hardly detectable; on the other hand, they can be confused with technological issues. In addition to that, fair players do not have full access to information about cheats, as the sources available are indirect or inaccessible. All these elements contribute to making cheating an evanescent, indeterminate, and uncertain phenomenon, whereby it is difficult to understand who the cheaters are, what kinds of cheats they use, and whether players are really facing a cheater behavior during a game session. As a consequence, many players share in-game experiences against cheaters, which can be summarized with the question, "*is it legit, to you?*," meaning that their aim is to gather the others' opinion about the way they were killed and reach a judgment about the presence of a cheater in the game.

In conclusion, players differently set boundaries between cheating and co-related phenomena and have varied degrees of knowledge about the technical aspects of cheats and their functioning, which is mostly derived from indirect experience. Uncertainty of cheating is also profoundly tied to the sophistication of hacks and, therefore, to the difficulty in recognizing unfair players. Still, detecting cheating behaviors is important, because this may change the players' perception of the game events.

4.2 Playing a "Good Game": competence and cheating identification practices

The ethnographer's personal experience made it clear how being good at playing is pivotal in a game like Warzone. Competence is so diriment that the ethnographer was pushed to train herself, level up her weapons, and study how to ameliorate her aim in order to take part in the matches with the most experienced players. This theme, therefore, is grounded in this first-person experience: the ethnographer investigated first-hand the importance of competence in the game and its role in the detection of cheaters, also interviewing and talking informally with other players, and analyzing several Facebook posts and videos about the matter.

4.2.1 What is competence for players

Being good at playing depends on the *resources* allocated to the game. First of all, the *economic resources* invested in the game are crucial, since money, as we have seen, can buy the best-performing hardware: some hardcore gamers declared to purchase valuable technological equipment with the intent to augment their skills, as P17: "*As far as I know, players could be equipped with good reflexes and the ability to control eager emotions but having the right devices can make the difference*." For instance, good headphones improve audio quality, which means that hearing the steps of the enemy approaching should be easier, as well as having a suited monitor might support quick detection of opponents. Money can also be used in-game to unlock the most powerful weapons (or *meta weapons*, in jargon) and mimetic skins. Nevertheless, economic resources do not grant players a "real" competence, which instead relates to the *temporal resources* devoted to the game. Playing skills are the outcome of the player's dedication and perseverance: as the ethnographer experienced during the fieldwork, time spent learning how to move the avatar within the game arena, aim the target, control the weapons, and use killstreak rewards is essential. These fundamental skills are paramount to distinguish a cheater from a (fair) experienced player, whose exceptional performance cannot be attributed to the use of hacks.

4.2.2 Competence and cheat recognition

Competence is also an essential factor that influences the players' accuracy in the identification of cheaters, differentiating novices/average players, master players, and streamers/pro players in their capability of detecting cheating behaviors. These differences clearly emerged from the analysis of the data collected through the semi-structured interviews and of the videos displaying the streamers' performances.

4.2.2.1 Novices and average players. By and large, less competent players have limited criteria to recognize cheaters and report few "certain" encounters with them (P1, P11), despite

considering cheating to be "out of control" in Warzone's world. With a few exceptions, novices and average players report vague and generic reasons for suspecting a player to be a cheater, e.g., "*I was killed way too easily"* (P9) or *"I was too far from the enemy to be killed"* (P8). These players highlight that they often felt uncanny sensations when they encountered a potential cheater, as the player under scrutiny had a sort of nonhuman behavior. Often this sensation is permeated by doubts, so that they can almost never be sure that they have encountered a cheater. In fact, this feeling may merely emerge from a suspect, as in the case of P8, *"Once I happened to think that a companion could be a cheater… basically he had a strange modus operandi… and, most of all, he was too big for his britches*,*"* which makes the detection of cheating much more a matter of belief and supposition than knowledge and certainty. Novices and average players also have less familiarity with technological aids (e.g., kill-cam, replay) that may help them analyze the moments before their death and understand how they were killed, with what gun, and at what distance: this information may be essential to identify a cheater, and not having the competence to use it may undermine the players' capability to recognize cheating behaviors.

4.2.2.2 Master players. Most expert participants showed to have a large toolbox to detect a cheater, grounding their opinions on direct experience and knowledge. We may classify the criteria that they employ along three main categories: i) using the game knowledge that they developed over time; ii) comparing the potential cheater with a "model" of the player; iii) using statistics and metrics.

First, expert participants appear to have internalized the rules governing the game, which shape a variety of expectations about the game functioning, even in its smallest details: "*If you have a Kilo* [type of weapon] *the time-to-kill is shorter… this means that you need less time to kill an opponent, because the weapon… while, if you use AK*-47 [a type of weapon]*, unless you are very good at controlling it, there's the recoil, so not all the bullets will shoot… in case a cheater is using*

no recoil with this weapon, then it will be easier for her to reduce the time-to-kill, but this is inconsistent with the weapon she is using." (P6). Masters' knowledge also entails expectations about the key dynamics of the game, i.e., what events should occur at a certain point of the battle. For instance, it will take a certain amount of time for all the squads to be eliminated. Periodically, an automatic message informs the players about the number of opponents that are still in the running. Therefore, if after a relatively short time the message announces that there are only a few players alive, this may mean that there are one or more cheaters who are eliminating the adversaries with great ease.

Secondly, expert players commonly build a "normative model" of the player, namely, they have clear in mind those characteristics that make a person a "good player": such a model is often used as a means of comparison to identify a cheater. In fact, also pro players' gunfights might have some flaws, and this is what makes them human: they might miss some shots or not perfectly keep the aim on the target. Conversely, players who use hacks do not make aim mistakes but still lack the most "human" strategic skills: they have a sort of machine-like ability, which makes them almost unbeatable but incapable of thinking and reacting in uncertain situations. Instead, players who rely only on their "natural" abilities are nimble, and their knowledge of the battlefield can be used to defeat the cheaters themselves, as P10 explains: "*There is this streamer I have been following for a while, well… when he believes there's a cheater in the lobby he takes a shield and some flashbangs… he gets close to the cheater to stun her and disable the hacks, so the cheater doesn't know what to do anymore… then he kills her easily with a gun… because a cheater doesn't know what to do in a difficult situation, he's clunky and clumsy*."

Finally, expert players look at the data that display a player's performances and mainly analyze their consistency, by comparing the information about her game experience (e.g., the overall time spent in the game) with that indicating her skills, in particular the K/D or the game level. This practice is particularly evident in P6's words: "*If a player has 5 K/D and only 30 victories he clearly has a new account… it's not possible… normally only pro players or streamers*

have such a high K/D, so you expect them to have, let's say, 1500 win, a high level of Prestige… if a player with no Prestige, a new account, a high K/D, headshot percentage 50% and killed you badly… something is wrong with him."

4.2.2.3 Streamers. Streamers have a high level of competence about Warzone. As they are recognized by their followers as the "experts" and "paladins" of the game, they are often engaged in identifying cheaters among the other streamers. To do so, they look for a variety of cheating "clues," scrutinizing the other streamers' avatar behavior.

A first group of clues concerns the technological aspects of cheating. Some cheats might be spotted just by looking at the way the weapons function (e.g., how the target is aimed and held in place), but to make them more apparent, the gunfight is analyzed in slow motion. As can be seen in the video "*How to recognize a cheater*," a popular streamer explained: "*Are you familiar with the so-called flick-shot? It is when you rapidly shoot your target… well, there are no frames between a shot and another… while normally there are at least five or six… this is easily detectable if you put the clip in slow motion*." The analysis of the visual and auditory aids at disposal of the player is also important: a cheater using a *wallhack* typically shoots the enemy before she is visible from the observer's perspective (*pre-fire*).

Moreover, streamers compare the behavior of the possible cheater with the behavior that she would have performed if she was actually skilled. In this sense, streamers show to have in mind a model of the "good player" – similarly to the master players. This model may be seen as composed of a series of unwritten rules about what should be done and not done in certain situations. A model being breached many times during the gameplay constitutes a yellow flag. For instance, a video of the series "*Peanuts and Cheaters*" thoroughly puts under scrutiny the gameplay of an unfair player, which is detectable by the fact that she ignores the squad indications (*ping*) about the position of an enemy or possible resources within the area, as if she had more detailed information or did not believe that the team play could make any difference; she engages in a firefight before checking to

have a full armor protection, as she does not need them; she runs into the possible location of a group of enemies without looking for the most secure path.

To summarize, competence is a relevant factor in shaping players' perceptions about game cheaters and deeply affects how they identify hackers.

*4.3 **The consequences of cheating***

The elaboration of this last theme is deeply informed by the interviews and the reflections that the ethnographer made in relation to the gaming sessions that she played, when she paid attention to the emotions expressed by the members of her team and the communicative exchanges occurred during the battles. The detailed analysis of the recorded gaming sessions that the ethnographer played helped her interpret how the players' beliefs about cheating (e.g., when they were supposedly killed by a cheater) were connected to their emotional states and behaviors. The analysis of the gaming sessions broadcasted by content creators and streamers further enriched the theme.

4.3.1 Frustration, anger, suspect: fostering paranoia

Despite cheating in Warzone is an "evanescent phenomenon" its effects on the players' experience and practices are real. Almost all the participants declared to experience negative emotions ranging from astonishment, frustration, and rage when they only suspect the presence of a cheater in the game arena. Some players also said that they suffer from the negative mood that permeates the air when an episode of cheating is believed to be happened: "*When my friends start questioning the way they were killed, I know that the match will be ruined… because some of them will start to rage, to be unfocused… and I can't stand it*" (P3).

By the same token, some players believe that the fear of encountering a cheater is pervasive to the point of ruining the game experience. Several players recounted that they received accusations of using hacks (*hackusation*, in the game jargon), right after winning a gunfight against an opponent: this was perceived as a way to discredit their win. Since the cheat reporting system of

the game gives players the possibility to report any abuse, it paves the way for those who want to take revenge after a defeat, as shown by P15: "*my profile has been banned because Activision said I was using cheats... I don't know where they got this data from* […] *another explanation is that I was reported many times by people who did it in a moment of despair or frustration... that's why I think constant reporting is unproductive and does no good... it's crying wolf… My friends do this too, they report players when they are killed just because they are frustrated*."

A few participants suggested that accusing others of cheating is the result of harsh competitiveness, envy and toxic dynamics occurring within the community: to cry "*hacker*!" after being outplayed might be a way to justify personal incapacity and rework negative emotional states provoked by the defeat, thus providing players with a safety valve to blow off. As recounted by P7: "*I can't count the times I heard someone accusing me of cheating… it makes me laugh… they are just people who refuse to be defeated*." However, a pervasive suspect may be detrimental for interaction among fellow players and even expose fair players to unnecessary sanctions. Social dynamics occurring within the community may then be impaired due to the rising of a culture of suspicion or even "paranoia."

Firstly, at local level, players might be suspicious not only of players in the enemy team, but also of the members of the squad/regiment to which they belong: "*To me, he* [anonymized] *uses cheats… it's not possible, I played with him, and he always knew where enemies were… up until the other day he was a noob and now he's so confident*" (P16). Since players ignore the actual functioning of the game reporting system, they might exclude suspected cheaters from their own regiment or playing team for the fear of being banned, as if they could be somehow "contaminated" by them: "*I once played against an Italian team, where there was a cheater… and the cheater helped them win… and at the end of the game, the rest of the team apologized, saying that the cheater was a random player for them and that they couldn't imagine… but those who play with cheaters risk a lot, because Activision may even ban them*" (P15).

Secondly, at the level of the broad community, there is a quite common belief that everyone uses some sort of hacks, as also told by P16: "*In my opinion amateur players like me play in lobbies made up of more than a half of cheaters… even if not everybody has all the cheats, they at least use aimbot or wallhack*."

Thirdly, at the institutional level, players blame the publisher's inactivity and produce "conspiracy theories" about the possible involvement of the company in the cheating phenomenon. An example is offered by P14: "*In my opinion the cheats always come out from Activision… they are always the ones that sell them through third-party sites, but at the end of the day they are always the ones who earn in the end*." As time passes without the issue being solved, such theories inevitably self-reinforce. In fact, despite the great number of accounts that have been banned, the problem is still there.

In October 2021, an anti-cheat automated solution called Ricochet was released by the company, but the situation appears still problematic. According to players, Ricochet was effective for a couple of weeks, but then cheats' vendors managed to get around it, or, alternatively, Activision Blizzard itself "*did not want to give up its profits coming from selling cheats*" (P14). Again, the players' perception of the phenomenon is built on multiple, even contrasting sources and rumors: while some of these players regained confidence in the gaming company, others think that there are no possible remedies to cheating.

4.3.2 The emergence of a surveillance culture

As a valid anti-cheat has not been released for a long time and still appears not to be resolutive, players can only rely on peer-to-peer reporting and, therefore, on their ability to recognize cheaters. However, an unequivocal identification of cheaters is hard to reach, as information about cheats is uncertain and the players' judgment can be biased. The pervasive suspect may culminate in a sort of "surveillance culture," which differently characterizes the amateur players, who mostly play for fun, and the streamers, who aim to make gaming a sort of "work."

4.3.2.1 Amateur players: observing to regain agency and control. Amateur players have little chance to manage the consequences of playing against dishonest gamers, having trouble in recognizing the cheaters and ignoring how to defeat them. In particular, only few amateur players (the masters) used strategies to actively fight cheaters, while the majority of participants reported a more "passive" response, avoiding cheaters or even leaving the match: "*If I am sure* [there is a cheater] *I usually quit the match"* (P16). Others recount that they make a cognitive and emotional adjustment by lowering their expectations about the possibilities of victory or reworking the value of a defeat at the end of the match, as P1 explains: "*We ranked second… and to me it's like we've won... the fact that they killed us does not matter to me, because it doesn't depend on the skills*."

This sense of powerlessness and the passive acceptance of cheating, however, often foster the need to regain a sort of agency and sense of control over cheaters: several players utilized a strategy that may counterbalance this asymmetry, thoroughly observing other players' behavior by exploiting certain game design features. The so-called *KillCam* shows for about 5 seconds a player's death from the first-person perspective of the killer, so that players may locate the position of the enemy and identify possible cheaters by, for example, assessing the distance from which the enemy shot: "*Once I was killed but I couldn't understand how, I thought not to be visible* [to the enemy's eyes]*... so I thought there was a cheater… then, looking at the KillCam, I noticed that I was in fact very visible!*" (P3).

Moreover, when an entire squad is defeated, its members still have the possibility to observe the rest of the match from the perspective of one of the enemies who is still in game, i.e., in spectator mode. In that case, the icon of an eye and the number of spectators appears on the interface of the observed player. Such observations are almost always conducted with the objective of judging the enemies' fairness, as P1 recounts: "*I warned the others that something was wrong, I said,* '*Hey guys, wasn't there a wall* [between the enemy and the player]*?' Because they were too focused on the game… and then, when they saw the replay they said, 'yes, it's true!'... I first noticed because I had died, so I could spectate*".

Alongside, players who are spectated by the losing teams are aware that the audience is driven by the willingness to control rather than to have fun. This produces a state of continuous surveillance, whereby every in-game action can be always scrutinized, and each player may become an observer as well as a person observed.

4.3.2.2 Streamers: observing to maintain reputation. Even though cheating may be tolerated in certain circumstances, it is absolutely inexcusable when it is performed by people who make gaming a sort of work, like the streamers. Almost all the participants defined the streamers' cheating a deception, because they would betray the trust of their followers: "*if you cheat when there are people who follow you, who talk with you, who believe in you* […] *taking advantage of the people who support you, who pay for your food ... I am happy that these people were denounced because they were taking advantage of those who believed in them"* (P6). As streamers' career and fame is built on their own gaming performances, their followers believe to have valid reasons to analytically observe and assess their in-game actions: as a result, streamers are subject to a constant risk of being reported or accused of cheating.

Hackusations, however, may also be used by the streamers to minimize the value of their own defeats and protect their public image. Nonetheless, wrong accusations might make streamers appear as people devoid of sportsmanship who look for a cushy backdoor for their poor gameplay. In fact, players expect streamers to use their expertise to produce accurate identification of cheaters. As an example, a streamer having more than 100,000 followers was killed during a live stream by an opponent, who was immediately reported as a cheater by him. When it was clear that the hackusation was wrong, he ironically said that "*Because we* [streamers] *are smart aleck, it's normal bro… we have dignity and a name to defend… I can't be killed and admit that the other player was better than me… Every time I die, I must say something like 'he's a cheater' or 'he's a camper*'." Unfortunately for the streamer, the whole event was recorded, and his reputation was dramatically impacted.

The climate of mutual suspicion and the opportunity to use such suspicion as a "weapon" against others result in many streamers engaging in reciprocal accusations, where both parties attempt to produce evidence of the other's unfair behavior. Moreover, players see streamers as watchmen of public order and ambassadors of the community, so they may feel responsible for discovering unfair competitors.

This results in continuous reciprocal observations, which become materialized in videos, produced by the streamers and followed by the game community, thoroughly analyzing the others' gameplay in its smallest details. This practice is sometimes taken to the extremes, as observations may concern the body of the person: the movements that she makes on the keyboard, the hand-eye coordination, the direction of the gaze, and so on. For instance, in one of these videos, a player was accused to move his head constantly, as he were looking at a possible hacking application located on a possible second hidden screen. The only solution for a streamer who ends up being "hackused" in this way is to record herself while playing to deflect suspicion: for instance, after being "blackmailed" by two players, one of the most popular Italian streamers decided to record his playing sessions with a camera.

In sum, cheating has negative effects on both amateur players and streamers but solutions to contain the phenomenon are scarce and mostly grounded on peer-to-peer reports. In this situation, amateur players perform observational practices, which produce a state of pervasive social surveillance. Likewise, streamers seem to be immersed in a panopticon culture even to a greater extent than amateur players.

5. Discussion

The goal of the present study was to describe how cheating afflicts the whole gaming ecosystem of COD: Warzone, giving an answer to the following research question: How do different players perceive and make sense of the cheating practices performed in their gaming environment? With this aim, we explored the players' subjective perceptions of and beliefs around cheating in

Warzone, highlighting how they understand the phenomenon, how they attempt to determine the presence of cheaters, and the effects that such beliefs and understandings have on the gaming community. In the following, we discuss the three main contributions of the study: the definition of cheating as a contextual phenomenon, which also depends on the players' socio-material conditions and the "role" of the cheater; ii) the conceptualization of cheating as a black box, being characterized by a profound uncertainty; iii) the design implications that can be derived from our findings.

5.1 Cheating as a contextual phenomenon

A key finding of this study is that cheating is a multifaceted and contextual phenomenon, the perception thereof depends on the players' competence in playing, as well as on their socio-material conditions and the "role" that the cheater has in the game community. Players of Warzone are not equal because they can allocate different temporal and monetary resources to the game. Players who can spend a huge amount of time in the game develop in-game skills that allow them to correctly identify the cheaters, while novices and average players tend to rely on their "feelings," which are much more imprecise and often result in unsubstantiated suspects and biased perceptions of the phenomenon, as we have seen in Section 4.2.

Moreover, players' technology equipment incorporates the non-equal distribution of monetary resources, and thus power, across players, representing a social stratification that undermines "fair competition." In fact, in Warzone social recognition and personal growth can be obtained only at great (even monetary) expenses. This contrasts previous findings on video games that entail complex social dynamics, like World of Warcraft (WoW), where players feel that everyone can be recognized for their abilities and feel to be the agent of their own progress (Rapp, 2017, 2020). For this, certain Warzone players may consider buying expensive game hardware a way to cheat, while others, who hold greater monetary resources, may see this practice as perfectly legitimate, as we noticed in Section 4.1.2.

Additionally, players' accounts of cheating are bound to the practices in which cheating is performed: when such practices are assimilated to real-world working practices (like professional sports and social media influencers as it happens for professional players and streamers), where individuals can obtain real-world advantages from their dishonest gaming actions, cheating is considered as an injustice that needs to be eradicated to reestablish trust. Instead, when it is performed by amateur players, the cheater may become a source of danger for the actual experience of play, which needs to be discovered for not contaminating the other players, or even someone that can be tolerated provided that he has the competence to play the game (see Section 4.1.1).

A first contribution of this study, therefore, is an original in-depth account of cheating that describes it as contextual, thus confirming previous research highlighting that there is no consensus on the specific behaviors that are considered unfair by players (Yan & Choi, 2002; Consalvo, 2005a, 2007). However, we extend the conceptualization of cheating as a contextual phenomenon, by connecting the players' diverse accounts of cheating practices in relation to their socio-material conditions and the different "figures" that characterize the game world, which have been neglected by previous research. In so doing, we also illustrated the different strategies that such different figures, which may hold different level of "competence," may utilize to identify and counteract cheaters: this aspect, which revolves around the competence and criteria needed to assess the culpability of players, has been ignored by previous research (Steam, 2021).

5.2 Uncertainty: cheating as a black box

Another key finding of this research is that cheating is characterized by uncertainty, meant as the inability or impossibility of part of the players to know in depth the functioning of hacks and therefore to correctly recognize those who use them in the game. Here, technology profoundly contributes to increasing the uncertainty of the cheating phenomenon. The essential role of uncertainty in cheating emerging from our findings leads to a novel conceptualization of cheating as a black box, i.e., a phenomenon whose existence can only be inferred by means of cues that only a

restricted elite of players is seemingly able to identify and that, nonetheless, produces "real" effects on all the players: this represents our second main contribution. The impossibility to correctly estimate the nature and diffusion of this practice and to perform a clear detection of cheaters during a match yield several consequences that invest the community at large. In the next subsections, we unfold the role of uncertainty and its emotional, sense-making, and social consequences, as they emerge from our findings.

5.2.1 Stress and emotion regulation: emotional consequences of uncertainty

Uncertainty can be partially explained by the technological characteristics of cheats – whose software is designed to make the practice less identifiable as possible (Jonnalagadda et al., 2021). More experienced players may overcome the opaqueness of cheats, but the majority of players do not hold sufficient competence and may either believe that cheaters are responsible for most of their negative experience of play or use hackusations as a strategy for seeing themselves in a more positive light. In both cases, this uncertainty produces important emotional consequences.

On the one hand, continuous loss, repeated deaths, and few wins may easily pave the way for frustration, as we have seen in Section 4.3.1. Previous research already acknowledged that the violent and competitive nature of the Battle Royale genre may expose players to frustration and act as a potential trigger of stress (Ohno, 2021; Kaye & Bryce, 2012). Adding to this, when amateur players perceive that their efforts to attain a certain objective are vain because they might be illegitimately defeated by others, they may respond with anger and express aggressive feelings (Baron & Richardson, 1994; Folger & Baron, 1996). The same applies for streamers and professionals who spend their time in the game in search of an economical return.

On the other hand, accusing others of performing unfair play may help amateur players rework their negative emotions resulting from the loss of a match. This finds confirmation in previous works, which concluded that assigning culpability is vital to alleviating the emotional turmoil that arises when a person perceives to be victim of an injustice (Walker, 2006). Reframing a

failure as a non-event by accusing the opponent of using hacks is an example of cognitive reappraisals, which aim to transform the evaluation of a situation to modulate the negative feelings that it may engender (Gross, 1998): there reappraisals are very common in Warzone, even among streamers, as we noticed in Section 4.3.2.2.

Blaming others for playing dirty might thus have a positive emotional effect for players, but at the same time it may have unwanted side-effects: being identification of cheaters uncertain, aggression might be directed towards any target, fair players included. In fact, as people tend to reciprocate the aggression received, similar behaviors may spiral upward (Ohbuchi & Kambara, 1985), thus contributing to exacerbating the aggressiveness and toxicity of the gaming environment.

5.2.2 Sense-making: how uncertainty sustains the production of (unfounded) meanings

As cheats are difficult to detect, most players are involved in a constant interpretative process, aimed at understanding whether the enemy is fair, namely, whether her victory is due to "human" abilities or illegitimate aids. Players who do not have in-depth knowledge of the cheating dynamics continuously attempt to produce correct interpretations of the phenomenon by gathering, sharing, discussing information coming from different indirect sources, as we have pointed out in Section 4.1.4: conversations with fellow gamers, content and news published on social media and channels dedicated to the game. However, as it happens in other situations that appear ambiguous, such as crisis events (Kou et al., 2017; Boldi et al., 2022), players may be exposed to rumors, a form of communication through which people try to make meaningful interpretations of what is happening (Shibutani, 1966). In the case of Warzone, this continuous sense-making activity based on unreliable sources contributes to making the phenomenon even more evanescent and fueling the spreading of further uncertain information.

Uncertain interpretations, fueled by the belief that unfairness proliferates with no control, may entail the belief that every in-game action is contaminated by cheating. In this sense, it may insinuate the doubt that even the fellow players are cheating, as well as the publisher and the game

developers, eventually producing a variety of conspiracy theories, as we noticed in Section 4.3.1. Similar narrations – that are allegations "of misconduct committed by a powerful group" (van Prooijen & Vries, 2016, p. 480), easily emerge in complex and distressing reality (Abalakina-Paap et al. 1999) and when people have feelings of powerlessness (Hofstadter, 1965). It may sound reasonable that similar theories are more than the expression of a simple distrust towards the game company but represent a means to make sense of the situation, offering a simple explanation to a complex problem (Zonis & Joseph, 1994).

5.2.3 Surveillance: the social consequences of uncertainty supported by technology

In an environment characterized by uncertainty, it is easy to witness the emergence of "investigative" practices among the population, which are normally aimed at making sense of the events, by analyzing others' intentions and motives (Kramer, 2001), or at reducing uncertainty and regain control, similarly to what happens during crisis or catastrophic events (Heverin & Zach, 2012). In Warzone, such control takes the form of social surveillance, as we explained in Sections 4.3.2.1 and 4.3.2.2, which consists in a decentralized and reciprocal controlling activity (Marwick, 2012). Depending on the role played in the community, observation and control are performed in a more or less formal and structured way. For certain streamers, control may take even the form of a "job," whose claimed mission is to contain the diffusion of the phenomenon and to share a body of knowledge around cheating that could help other players recognize unfair individuals.

Of course, in a game social control can be performed only if technology permits it, which is the case of Warzone, within which social surveillance is enabled by a number of design choices that allow: i) first-perspective observations of the others' gameplay; ii) the reporting of behaviors that break the norms of the game; and iii) the analysis of performance through public statistics, as we highlighted in the recount of the findings. The presence of these design features may be read as the attempt of the gaming company to patch up the problem by relying on reciprocal monitoring, whereby top-down solutions are neither sufficient nor effective.

In fact, as highlighted by Jonnalagadda et al. (2021), manual inspection of gameplay and voluntary reporting of other players are currently the most effective approach to block cheating. However, such an approach may lead to a state of pervasive surveillance and "paranoia", where players may be unfairly hackused and be pervaded by the fear of being banned from the game. These negative consequences of reporting may be the effect of the combination of the game design features enabling the control of the players' behavior with the gaming practices that they perform to manage uncertainty: for example, their continuous attempts to make sense of the others' gameplay, to gain information from a variety of (unreliable) sources, and to emotionally cope with their (possibly unfair) losses, which all have been pointed out by our study. A technical solution that considers such practices should then acknowledge that players often do not hold enough knowledge to perform correct reporting and that their judgment may be biased by emotional factors and influenced by the collective perception of the phenomenon.

5.3 Implications for design

The third contribution of our research is to propose three design implications emerging from the study findings, which could be applied in those video gaming contexts that are plagued by the spreading of cheating practices and cannot be controlled by the absolute reliance on technological solutions.

5.3.1 Encourage information dissemination and knowledge among players

Part of the problem associated with cheating depends on the asymmetric distribution of information, whereby more experienced players seem to be able to decipher ambiguous situations in more effective and accurate ways with respect to inexperienced players. However, even the most experienced players and streamers may produce inaccurate hackusations, if these hackusation allow them to emotionally shield themselves from a defeat or to protect their public image. Currently, cheating-themed content is mostly produced by the players themselves, while the institutional

presence, i.e., the game company and developers, is rather sparse. This absence can lead players to generate conspiracy theories about the company's involvement in the phenomenon.

To fill this void, the gaming company could: i) create specialized content and guides that could help juggle the material circulating online, the sheer quantity of which risks confusing and discouraging anyone trying to better understand the topic; ii) help players classify the quality of the content found online: drawing from literature addressing misinformation on social media by means of web add-on corrections (e.g., Lee, 2022), such materials might be "flagged" to indicate the quality of the information; iii) leverage the influence of streamers by building partnerships with those who are popular and particularly engaged in the battle against unfairness, and create social networks where reliable information about cheating is conveyed by such public figures. The goal of such solutions would be, on the one side, to rebuild trust and social order, by reducing the asymmetries and the distance between the players and those who occupy positions of high power and status (see Kramer, 2001), namely the publisher and the developers; on the other side, to contrast the flood of false information by offering a solid guide.

5.3.2 Augment transparency of technological solutions

Warzone's ban system based on the players' reports has unclear criteria and follows a completely opaque process. Players of League of Legends are subjected to a similar condition, as punishments for toxic behaviors are guided by an Artificial Intelligence (AI)-moderation system, whose functioning has not been explained by Riot Games (Kou et al., 2017). Considering the growing attention to issues of accountability of AI systems and the rise of explainable AI (Mittelstadt et al., 2018), it is important for the game companies to improve the transparency of the systems and methods used for tackling cheating behavior, by undercovering the criteria that determine in what conditions the activity of a player is scrutinized and what the player can do to avoid such situation. Players could be allowed to review the game actions that led to the report and be prompted with data that may "objectively" signal possible unfair actions (e.g., an excess of kills).

Augmenting transparency would increase users' perceived trust and fairness (Lee et al., 2019), and hopefully help to contrast the climate of rampant suspicion. As found by Kou and Gui (2020), when the reasons behind a punishment are not clear, players seek explanations within the gaming community. Activision may then provide players with a space, i.e., a forum, where issues around punishments are openly discussed with other players, as well as with developers and designers. Finally, customer service professionals, even in the automated form of conversational agents, could be trained to explain to the players the reasons that led to the ban, responding accurately to their requests for clarification.

5.3.3 Integrate technological and human solutions

Being absent a valid solution to cheating, players have taken full advantage of the design possibilities offered by the game to counteract cheaters, observing other players during the game sessions, examining their game statistics, and finally reporting them. This peer-based reporting system can be effective as a complement to a technological solution. However, players are not always able to do proper reports or may be driven by anger, which may bias their judgment. This approach may then expose the game company to the risk of banning fair players, exacerbating the feeling of unfairness within the community: players may also be afraid of a punishment system that is perceived as unreliable.

To limit unfair reporting, we suggest that the interaction with the system is "slowed down," in line with the principles of "slow technology" (e.g., Odom et al., 2012), so as to encourage reflection and avoid rushed judgments. A slightly similar approach has been employed by Ubisoft, for the FPS Tom Clancy's Rainbow Six Siege (Ubisoft, 2022). For example, as the player reports a suspected cheater, she may be recontacted later to finalize the reporting: this time delay would limit those reports triggered by negative feelings, at the same time stimulating people who are truly motivated to finalize the hackusation. A section asking about the reasons for reporting could also be added, so that the player may have the possibility to explain her motives and possibly attach

screenshots of the gaming sessions as a probe. The goal is to stimulate players to think about the legitimacy of their reporting.

Another possibility to limit relentless mutual surveillance would be to evaluate the accuracy of single reports comparing them with the feedback given by automatic systems. Reports might be rated in terms of accuracy and be stored among the statistics of the player – as a social deterrent for false hackusations. In line with the human-in-the-loop approach, according to which people are involved in the improvement of artificial intelligence systems (Kamar, 2016), this constant comparison might also help the developers adjust and correct their systems, which may learn from human judgments through a constant feedback loop.

6. Limitations

Methodological limitations should be considered. Deciding to collect data within the Italian community might have affected the collected results, as players located in different world regions could conceive the game and cheating practices in a different way. On the other hand, the research took place in specific "seasons" of the game: despite the publisher maintaining untouched the core game mechanics, slight differences in the design features of the different versions of the game may alter the game experience. Therefore, the findings reported in this article may not find full confirmation in further evolutions of the game. As we opted for an in-depth analysis of a single game, the findings of our study may not be generalizable to other video games. Future studies may then explore how cheating unfolds in other games and analyze how the phenomenon varies depending on the characteristics of the video game, such as the genre, the content of the game, and the size of the game community. Research could also investigate how different motives for playing, as well as the perception of playing either as a "work" or a leisure activity, can influence people's aversion or propensity to cheating. The well-being and the level of stress related to the constant monitoring of streamers and professional players could also be explored in the future.

7. Conclusion

Research has made substantial efforts in exploring how cheating behaviors unfold in multiplayer video games, with the aim to limit the noxious effect that cheating has on the gaming experience. However, while technological approaches to cheating are not always available or effective in limiting the spread of unfair practices, human-centered perspectives underestimate the role of technology and not sufficiently consider the social complexity of contemporary gaming environments, which are populated by a variety of figures having different motives for playing.

In this article, we offered an exploration of both the technological and human aspects of cheating, based on a 9-month-long digital ethnography within Call of Duty: Warzone. We found that players' perception of cheating depends on their competence, their socio-material conditions, and the role of the individual who performs the unfair behavior. Moreover, as the knowledge of the cheating practices is fragmented and uncertain, the phenomenon becomes a sort of "black box," characterized by a profound indeterminateness. Amateur players are often prey to the others' opinions or rumors, while most skilled players seem to employ reasonable criteria to recognize cheaters in action. The harsh competitiveness characterizing the game paves the way for mutual "hackusations," which may affect both amateur players and streamers. Since Warzone offers design features that allow reciprocal observation and reporting, such a situation exacerbates the climate of paranoia and surveillance, leading to the consolidation of a toxic environment.

On the basis of these findings, we concluded the article with a set of design suggestions that could be used to address the issue of cheating in gaming environments entailing competitive dynamics: first, the gaming companies might encourage the dissemination of "right" information around cheating by leveraging the "power" of streamers; second, the transparency of the process that may make players undergo scrutiny may be improved; finally, peer-reporting systems may be redesigned in a way that encourages reflection and avoid rush decisions.

We hope that the insights recounted in this article could inspire future strands of research and attract the attention of those researchers who attempt to understand how dark behaviors originate and spread in large communities.

Declaration of interest statement

The authors report there are no competing interests to declare.

References

Aarseth, E. (2014). I fought the law: Transgressive play and the implied player. In *Proceedings of DiGRA 2007 Conference*. doi: 10.1057/9781137429704_13

Abalakina-Paap, M., Stephan, W., Craig, T., & Gregory, W. L. (1999). Beliefs in conspiracies. *Political Psychology, 20*, 637–647. doi: 10.1111/0162-895X.00160

Alayed, H., Frangoudes, F., & Neuman, C. (2013). Behavioral-based cheating detection in online first person shooters using machine learning techniques. In *2013 IEEE Conference on Computational Intelligence in Games (CIG)* (pp. 1-8). IEEE. doi: 10.1109/CIG.2013.6633617

Anderson, C. A., & Dill, K. E. (2000). Video games and aggressive thoughts, feelings, and behavior in the laboratory and in life. *Journal of Personality and Social Psychology, 78*(4), 772–790. https://doi.org/10.1037/0022-3514.78.4.772

Anderson-Coto, M. J., Tomlinson, C., Collado, J., Squire, K. (2019). Fandom Culture And Identity In Esports. In *Esports Research Conference* (p. 3). doi: 10.1184/R1/12217766

Ashton, G. (2019). Cheating in Esports – How Is It Done, and How Is It Dealt With? Accessed 5 January 2022. Retrieved from https://archive.esportsobserver.com/cheating-in-esports/

Bainbridge, W. A., & Bainbridge, W. S. (2007). Creative uses of software errors: Glitches and cheats. *Social Science Computer Review*, *25*(1), 61-77. doi: 10.1177/0894439306289510

Bandura, A. (1989). Social cognitive theory. In Vasta, R. (Ed.). *Annals of child development* (Vol. 6, pp. 1–60). Greenwich, CT: Jai Press Ltd.

Baron, R. A., & Richardson, D. R. (1994). Human Aggression, 2nd ed. New York: Plenum Press.

Blackburn, J., Kourtellis, N., Skvoretz, J., Ripeanu, M., & Iamnitchi, A. (2014). Cheating in online games: A social network perspective. *ACM Transactions on Internet Technology (TOIT)*, *13*(3), 1-25. doi: 10.1145/2602570

Blight, M. G. (2016). *Relationships to Video Game Streamers: Examining Gratifications, Parasocial Relationships, Fandom, and Community Affiliation Online*. Theses and Dissertations. 1255. https://dc.uwm.edu/etd/125

Boin, A., & 't Hart, P. (2007). The crisis approach. In H. Rodríguez, E. L. Quarantelli, & R. R. Dynes (Eds.), *Handbook of disaster research* (pp. 42-54). Springer, New York, NY. H.

Boldi, A., Rapp. A., Tirassa, M. (2022). Playing during a crisis: The impact of commercial video games on the reconfiguration of people's life during the COVID-19 pandemic. *Human-Computer Interaction*. doi: 10.1080/07370024.2022.2050725

Boluk, S., & LeMieux, P. (2017). Metagaming: Playing, competing, spectating, cheating, trading, making, and breaking videogames (Vol. 53). Minneapolis, MN: University of Minnesota Press.

Botvich, D., McGibney, J., Ostapenko, G., De Paoli, S., Kerr, A., & Keatinge, M. (2010). Integrating players, reputation and ranking to manage cheating in MMOGs. In *Proceedings of the Fifth International Conference on the Foundations of Digital Games* (pp. 17-24). doi: 10.1145/1822348.1822351

Bowen, G. A. (2008). Naturalistic inquiry and the saturation concept: a research note. *Qualitative Research, 8*(1), 137–152. doi: 10.1177/1468794107085301

Braun, V. & Clarke, V. (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. doi: 10.1191/1478088706qp063oa

Brock, T. (2017). Roger Caillois and e-sports: On the problems of treating play as work. *Games and Culture, 12*(4), 321-339. 10.1177/1555412016686878

Cardano, M. (2009). Etnografie: immagini della pratica etnografica. *Rassegna Italiana di Sociologia, 1*.

Ceyhan, A. (2008). Technologization of security: Management of uncertainty and risk in the age of biometrics. *Surveillance & society, 5*(2).

Chanda, S., Singh, T., & Star, S. (2021). Contouring E-doping: A menace to sportsmanship in E-sports.

CharlieIntel (2020, March 10). Again, in regards to matchmaking, Infinity Ward's studio head Pat Kelly told us that there is no skill based matchmaking in any large player count modes in Modern Warfare, and that will include Warzone. [Twitter post]. Accessed 21 July 2021. Retrieved from: https://twitter.com/charlieINTEL/status/1237386985871990785?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1237386985871990785%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.esportgaming.it%2Fblog%2Fcall-of-duty-warzone-sbmm-spiegato%2F

Chen, K. T., Pao, H. K. K., & Chang, H. C. (2008). Game bot identification based on manifold learning. In *Proceedings of the 7th ACM SIGCOMM Workshop on Network and System Support for Games* (pp. 21-26).

Chen, V. H. H., & Ong, J. (2018). The rationalization process of online game cheating behaviors. *Information, Communication & Society*, *21*(2), 273-287. doi: 10.1080/1369118X.2016.1271898

Chen, V. H. H., & Wu, Y. (2015). Group identification as a mediator of the effect of players' anonymity on cheating in online games. *Behaviour & Information Technology*, *34*(7), 658-667. doi: 10.1080/0144929X.2013.843721

Chui, C., Kouchaki, M., & Gino, F. (2021). "Many others are doing it, so why shouldn't I?": How being in larger competitions leads to more cheating. *Organizational Behavior and Human Decision Processes, 164*, 102-115. doi 10.1016/j.obhdp.2021.01.004

Circelli, R. (2021). Boosting and Reverse Boosting in Call of Duty Explained. Accessed 21 November 2021.Retrieved from: https://epicstream.com/article/valorant-agent-19

Coanda, I., & Aupers, S. (2020). Mechanisms of disclosure: a socio-technical perspective on sociality in massively multiplayer online role-playing games. *Television & New Media, 21*(3), 315-333. doi: 10.1177/1527476418824557

Collins, E., & Cox, A. L. (2014). Switch on to games: Can digital games aid post-work recovery?. International Journal of Human-Computer Studies, 72(8-9), 654-662. doi: 10.1016/j.ijhcs.2013.12.006

Conroy, E., Kowal, M., Toth, A. J., & Campbell, M. J. (2021). Boosting: Rank and skill deception in esports. *Entertainment Computing, 36*, 100393. 10.1016/j.entcom.2020.100393.

Consalvo, M. (2005). Gaining Advantage: How Videogame Players Define and Negotiate Cheating. In *DiGRA Conference*. doi: 10.7551/mitpress/1802.003.0008

Consalvo, M. (2007). *Cheating: Gaining advantage in videogames*. Cambridge, MA: The MIT Press.

Dailey, D., & Starbird, K. (2015). It's Raining Dispersant: Collective Sensemaking of Complex Information in Crisis Contexts. In *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing - CSCW'15 Companion*, 155–158. doi: 10.1145/2685553.2698995

Davis, J. P. (2002). *The Experience of 'Bad' Behavior in Online Social Spaces: A Survey of Online Users*. Social Computing Group, Microsoft Research.

Doherty, S. M., Liskey, D., Via, C. M., Frederick, C., Kring, J. P., & Liu, D. (2014). An analysis of expressed cheating behaviors in video games. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 58, No. 1, pp. 2393-2396). Los Angeles, CA: SAGE Publications. doi: 10.1177/1541931214581498

Dourish, P. (2004). What we talk about when we talk about context. *Personal and ubiquitous computing, 8*(1), 19-30. doi: 10.1007/s00779-003-0253-8

Duh, H. B. L. & Chen, V. H. H. (2009). Cheating behaviors in online gaming. In A. Ozok and P. Zaphiris (Eds.), *Online Communities and Social Computing* (pp. 567–73). Berlin, DE: Springer.

Dumitrica, D. D. (2011). An exploration of cheating in a virtual gaming world. *Journal of Gaming & Virtual Worlds*, *3*(1), 21-36. doi: 10.1386/jgvw.3.1.21_1

experiences of playing videogames. *International Journal of Internet Science, 7*(1), 23–37.

Feng, W. C., Kaiser, E., & Schluessler, T. (2008). Stealth measurements for cheat detection in on-line games. In *Proceedings of the 7th ACM SIGCOMM Workshop on Network and System Support for Games* (pp. 15-20).

Folger, R., & Baron, R. A. (1996). Violence and hostility at work: A model of reactions to perceived injustice. In G. R. VandenBos & E. Q. Bulatao (Eds.), *Violence on the job: Identifying risks and developing solutions* (pp. 51–85). American Psychological Association. https://doi.org/10.1037/10215-002

Gabbiadini, A., Riva, P., Andrighetto, L., Volpato, C., & Bushman, B. J. (2014). Interactive effect of moral disengagement and violent video games on self-control, cheating, and aggression. *Social Psychological and Personality Science*, *5*(4), 451-458. doi: 10.1177/1948550613509286

Galli, L., Loiacono, D., Cardamone, L., & Lanzi, P. L. (2011). A cheating detection framework for Unreal Tournament III: A machine learning approach. In *2011 IEEE Conference on Computational Intelligence and Games (CIG'11)* (pp. 266-272). IEEE.

Geertz, C. (1973). *The interpretation of cultures* (Vol. 5019). Basic books.

Goertzel, T. (1994). Belief in conspiracy theories. *Political Psychology, 15,* 731–742.

Gross, J. J. (1998). The emerging field of emotion regulation: An integrative review. Review of general psychology, 2(3), 271-299. 1089-2680/98

Gui, X., Kou, Y., Pine, K. H., & Chen, Y. (2017). Managing uncertainty: using social media for risk assessment during a public health crisis. In *Proceedings of the 2017 CHI conference on human factors in computing systems*, 4520-4533. doi: 10.1145/3025453.3025891

Hamlen, K. R., & Blumberg, F. C. (2015). Problem solving through "cheating" in video games. In *Video Games and Creativity* (pp. 83-97). Academic Press. doi: 10.1016/B978-0-12-801462-2.00004-7

Heverin, T., & Zach, L. (2012). Use of microblogging for collective sense-making during violent crises: A study of three campus shootings. *Journal of the American Society for Information Science and Technology*, *63*(1), 34-47. doi: 10.1002/asi.21685

Hofstadter, R. (1965). *The paranoid style in American politics and other essays*. New York: Knopf.

Holden J, Kaburakis A, & Rodenberg, R. (2017), The Future Is Now: Esports Policy Considerations and Potential Litigation. *SSRN Electronic Journal*.

Huizinga, J. (1955), *Homo Ludens*. Boston, MA: The Beacon Press.

Huseman, R. C., Hatfield, J. D., & Miles, E. W. (1987). A new perspective on equity theory: The equity sensitivity construct. Academy of Management Review, 12, 222–234.

Hussain, U., Jabarkhail, S., Cunningham, G.B., & Madsen, J.A. (2021). The dual nature of escapism in video gaming: A meta-analytic approach. *Computers in Human Behavior Reports,* 3, 100081. doi: 10.1016/j.chbr.2021.100081

Iacovides, I., & Mekler, E. D. (2019). The role of gaming during difficult life experiences. In *Proceedings of the 2019 CHI conference on human factors in computing systems* (pp. 1-12). doi: 10.1145/3290605.3300453

Irdeto. (2018). *Irdeto Global Gaming Survey: The last Checkpoint for Cheating*. Accessed November 1, 2021. Retrieved from: https://resources.irdeto.com/irdeto-global-gaming-survey/irdeto-global-gaming-survey-report-2.

Jonnalagadda, A., Frosio, I., Schneider, S., McGuire, M., & Kim, J. (2021). Robust Vision-Based Cheat Detection in Competitive Gaming. *Proceedings of the ACM on Computer Graphics and Interactive Techniques, 4*(1), 1-18. doi: 10.1145/3451259.

Kao, D. (2021) The effects of observation in video games: how remote observation influences player experience, motivation, and behaviour, *Behaviour & Information Technology*. doi: 10.1080/0144929X.2021.1906321

Kamar, E. (2016)- Directions in Hybrid Intelligence: Complementing AI Systems with Human Intelligence. In *IJCAI 2016*, Jul 9, pp. 4070-4073.

Kaplan, J. (2017). "Developer Update | Play Nice, Play Fair | Overwatch". Retrieved January 3, 2022. https://youtu.be/rnfzzz8pIBE.

Kardefelt-Winther, D. (2014). The moderating role of psychosocial well-being on the relationship between escapism and excessive online gaming. *Computers in Human Behavior, 38*, 68-74. doi: 10.1016/j.chb.2014.05.020

Kaye, L. K., & Bryce, J. (2012). Putting the "fun factor" into gaming: The influence of social contexts on

Knezovic, A. (2021). *Call of Duty Analysis: How It Shot to the Top and Stayed There*. Accessed 28 September 2021. Retrieved from: https://www.blog.udonis.co/mobile-marketing/mobile-games/call-of-duty-analysis

Koskinas, P. (2018). *Removing Cheaters from LoL*. Retrieved from: https://nexus.leagueoflegends.com/en-us/2018/10/dev-removing-cheaters-from-lol/. Accessed November 15, 2021.

Kou, Y., & Gui, X. (2020). Mediating community-AI interaction through situated explanation: the case of AI-Led moderation. *Proceedings of the ACM on Human-Computer Interaction, 4(*CSCW2), 1-27. doi: 10.1145/3415173

Kou, Y., Gui, X., Zhang, S., & Nardi, B. (2017). Managing disruptive behavior through non-hierarchical governance: Crowdsourcing in League of Legends and Weibo. Proceedings of the ACM on Human-Computer Interaction, 1(CSCW), 1-17. doi: 10.1145/3134697

Kramer, R. M. (2001). 1. Organizational paranoia: Origins and dynamics. *Research in organizational behavior*, 23, 1-42. doi: 10.1016/S0191-3085(01)23002-0

Kücklich, J. (2007). Wallhacks and aimbots: How cheating changes the perception of gamespace. In *Space Time Play: Computer Games, Architecture and Urbanism, Berlin: Birkhauser Verlag AG*, 118-24.

Kücklich, J. (2008). Forbidden pleasures: Cheating in computer games. In Swalwell, M. & Wilson, J. (Eds.), *The pleasures of computer gaming* (pp. 52–71). Jefferson, NC: McFarland.

Kücklich, J. (2009). A techno-semiotic approach to cheating in computer games: Or how I learned to stop worrying and love the machine. *Games and Culture*, *4*(2), 158-169. doi: 10.1177/1555412008325486

Kuecklich, J. (2004). Other playings: Cheating in computer games. In *Proceedings of the Other Players conference*.

Kühne, R., Patrick W., & Katharina S. (2015). Beyond Cognitive Framing Processes: Anger Mediates the Effects of Responsibility Framing on the Preference for Punitive Measures. Journal of Communication, 65, 259–79.

Kurz R., & Bartram, D. (2002) Competency and Individual Performance: Modelling the World of Work. In: I. T. Robertson, M. Callinan, D. Bartram (Eds.), *Organizational effectiveness: the role of psychology,* pp. 225–255. John Wiley, Chichester.

Laato, S., Rauti, S., Koivunen, L., & Smed, J. (2021). Technical cheating prevention in location-based games. In *International Conference on Computer Systems and Technologies' 21* (pp. 40-48). doi: 10.1145/3472410.3472449

Lankoski, P., & Björk, S. (2015). Formal analysis of gameplay. In P. Lankoski & S. Björk (Eds.), *Game research methods: An overview* (pp. 23–35). Pittsburgh, PA: ETC Press.

Laurens, P., Paige, R. F., Brooke, P. J., & Chivers, H. (2007). A novel approach to the detection of cheating in multiplayer online games. In *12th IEEE International Conference on Engineering Complex Computer Systems (ICECCS 2007)* (pp. 97-106). IEEE.

LeCompte, M. D., & Goetz, J. P. (1982). Problems of Reliability and Validity in Ethnographic Research. *Review of Educational Research*, *52*(1), 31–60. doi: 10.3102/00346543052001031.

Lee, J. (2022). The effect of web add-on correction and narrative correction on belief in misinformation depending on motivations for using social media. *Behaviour & Information Technology, 41*(3), 629-643. doi: 10.1080/0144929X.2020.1829708

Lee, M. K., Jain, A., Cha, H. J., Ojha, S., & Kusbit, D. (2019). Procedural justice in algorithmic fairness: Leveraging transparency and outcome control for fair algorithmic mediation. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), 1-26. doi: 10.1145/3359284

Lott, P. (2021). *Warzone: How Skill Based Matchmaking Works*. Accessed 8 December 2021. Retrieved from https://gamerant.com/warzone-skill-based-matchmaking-works/#:~:text=Technically%2C%20Warzone%20has%20what%20is,necessary%20to%20keep%20players%20interested

Marshall, M. N. (1996). Sampling for qualitative research. *Family Practice 13*(6), 522–526. doi:10.1093/fampra/13.6.522,

Marwick, A. (2012). The public domain: Surveillance in everyday life. *Surveillance & Society, 9*(4), 378-393.

Meades, A. F. (2015). *Understanding counterplay in video games*. New York, NY: Routledge.

Mittelstadt, B., Russell, C., & Wachter, S. (2019). Explaining explanations in AI. In Proceedings of the conference on fairness, accountability, and transparency (pp. 279-288). doi: 10.1145/3287560.3287574

Morris, S. (2003). WADs, Bots and Mods: Multiplayer FPS Games as Co-creative Media. In *Proceedings of the 2003 DiGRA International Conference: Level Up*. Available at: http://www. digra. org/wp-content/uploads/digital-library/05150.21522. pdf.

Mulligan, J., & Patrovsky, B. (2003). *Developing Online Games: An Insider's Guide*. Indianapolis, IND: New Riders Publishing.

Odom, W., Banks, R., Durrant, A., Kirk, D., Pierce, J., 2012. Slow technology: critical reflection and future directions. In: Proceedings of the Designing Interactive Systems Conference (DIS '12). Association for Computing Machinery, New York, NY, USA, pp. 816–817. https://doi.org/10.1145/2317956.2318088.

Ohbuchi, J., & Kambara, T. (1985). Attacker's intent and awareness of outcome, impression management and retaliation. *Journal of Experimental Social Psychology,* 21, 321–330.

Ohno, S. (2021). The link between battle royale games and aggressive feelings, addiction, and sense of underachievement: exploring esports-related genres. *International Journal of Mental Health and Addiction*, 1-9. doi: 10.1007/s11469-021-00488-0

Ortiz, S. M. (2020). Trolling as a collective form of harassment: an inductive study of how online users understand trolling. *Social Media+ Society, 6*(2). doi: 10.1177/2056305120928512

Paay, J., Kjeldskov, J., Internicola, D., & 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* (pp. 1-13). doi: 10.1145/3229434.3229466

Park, S., Ahmad, A., & Lee, B. (2020). Blackmirror: Preventing wallhacks in 3d online fps games. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (pp. 987-1000). doi: 10.1145/3372297.3417890

Parker, J. (2007). Cheating by video game participants. *Loading...*, *1*(1).

Pascoulis, J. (2021). *JGOD explains why Warzone players enjoy Rebirth Island more than Verdansk*. Accessed 30 November 2021. Retrieved from: https://charlieintel.com/jgod-explains-why-warzone-players-enjoy-rebirth-island-more-than-verdansk/137899/

Passmore, C. J., Miller, M. K., Liu, J., Phillips, C. J., & Mandryk, R. L. (2020). A Cheating Mood: The Emotional and Psychological Benefits of Cheating in Single-Player Games. In *Proceedings of the Annual Symposium on Computer-Human Interaction in Play* (pp. 58-70). doi: 10.1145/3410404.3414252

Patton, M. Q. (1990). *Qualitative evaluation and research methods*. SAGE Publications, inc.

Pekmic, A. (2021). *Is Warzone Dying? Player Count Shows Current State of the Game*. Retrieved from: https://www.vgr.com/is-warzone-dying-player-count-shows-current-state-of-the-game/#:~:text=Warzone%20player%20count%20and%20its%20popularity&text=As%20of%20this%20writing%2C%20Warzone,video%20game%20at%20one%20point. Accessed November 16, 2021.

Pellicone, A. J., & Ahn, J. (2017). The Game of Performing Play: Understanding streaming as cultural production. In *Proceedings of the 2017 CHI conference on human factors in computing systems* (pp. 4863-4874). doi: 10.1145/3025453.3025854

Polhamus, B. (2021). Why competitive Warzone can (not) work as an esport. Retrieved from: https://www.esports.com/en/why-competitive-warzone-cold-not-work-as-an-esport-216766. Accessed 3 December 2021.

Postigo, H. (2014). The socio-technical architecture of digital labor: Converting play into YouTube money. *New media & society, 18*(2), 332-349.

Powers, T. M. (2003). Real wrongs in virtual communities. *Ethics and information technology, 5*(4), 191-198. doi: 10.1023/B:ETIN.0000017737.56971.20

Rapp, A. (2017). Designing interactive systems through a game lens: An ethnographic approach. Computers in human behavior, 71, 455-468. doi: 10.1016/j.chb.2015.02.048

Rapp, A. (2018a) Social Game Elements in World of Warcraft: Interpersonal Relations, Groups, and Organizations for Gamification Design. International Journal of Human–Computer Interaction, 34(8), 759-773. doi: 10.1080/10447318.2018.1461760

Rapp, A. (2018b). Gamification for Self-Tracking: From World of Warcraft to the Design of Personal Informatics Systems. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18). ACM, New York, NY, USA, Paper 80, 15 pages. doi: 10.1145/3173574.3173654

Rapp, A. (2020). An exploration of world of Warcraft for the gamification of virtual organizations. *Electronic Commerce Research and Applications, 42*, 100985. doi: 10.1016/j.elerap.2020.100985

Rapp. A. (2021). In search for design elements: A new perspective for employing ethnography in human-computer interaction design research. *International Journal of Human–Computer Interaction*, 37(8), 783-802. doi: 10.1080/10447318.2020.1843296

Reinecke, L., Tamborini, R., Grizzard, M., Lewis, R., Eden, A., & Bowman, N. D. (2012). Characterizing mood management as need satisfaction: The effects of intrinsic needs on selective exposure and mood repair. Journal of Communication, 62(2), 437–453. doi:10.1111/j.1460-2455.2012.01649.x

Ribbens, W., Poels, Y., & Lamotte, G. (2011). Fail with honour or win by cheating? Research into the perceptions and motivations of cheaters in online multiplayer games. *Vice city virtue. Moral issues in digital game play*, 177-203.

Rode, J. A. (2011). Reflexivity in digital anthropology. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11), pp. 123–132.

Rojek, C. (1989) Leisure and the 'ruins of the bourgeois world', in C. Rojek (Ed.), *Leisure for Leisure: Critical Essays*, pp. 92–112. Routledge, New York.

Rosenthal, U., Charles, M.T., & Hart, P. (Eds.). (1989). *Coping with crisis: The management of disasters, riots and terrorism*. Springfield, IL: Charles C Thomas.

Saldaña, J. (2021). *The coding manual for qualitative researchers* (2nd Edition). Sage.

Salen, K. and Zimmerman, E. (2003). *Rules of Play: Game Design Fundamentals*. MIT Press, Chicago.

Schulzke, M. (2018). The politics of attributing blame for cyberattacks and the costs of uncertainty. *Perspectives on Politics, 16*(4), 954-968.

Sharma, R., Singh, G., & Sharma, S. (2021). Competitors' envy, gamers' pride: An exploration of gamers' divergent behavior. *Psychology & Marketing*, *38*(6), 965-980. doi: 10.1002/mar.21469

Shibutani, T. (1966). Improvised News: A Sociological Study of Rumor. Ardent Media. Accessed 26 November, 2021 Retrieved from: https://books.google.com/books/about/Improvised_News.html?id=zJypXrE2xqAC

Škrinjarić, B. (2022). Competence-based approaches in organizational and individual context. *Humanities and Social Sciences Communications*, *9*(1), 1-12. doi: 10.1057/s41599-022-01047-1

Skycheats.com. Best Call of Duty Warzone Hacks and Cheats to Enhance Your Gaming Experience. Retrieved from: https://www.skycheats.com/call-of-duty-warzone-hacks-cheats-aimbot-2021/. Accessed 11 December 2021.

Smith, H. (2006). Plans and purposes how video game goals shape player behaviour. [Doctoral dissertation, IT University of Copenhagen]. https://autofire.dk/wp-content/uploads/dissertation1-0.pdf

Snoeijers, M. (2018). *Organisational crisis communication and crisis perception: human factors and opportunities to strategies* (Doctoral dissertation, University of Antwerp).

Sonntag, K., & Schmidt-Rathjens, C. (2004). Competence models – Error factors in HR management?. A strategy and evidence-based approach to competency modeling. [Kompetenzmodelle–Erfolgsfaktoren im HR-Management?. Ein strategie-und evidenzbasierter Ansatz der Kompetenzmodellierung]. Personalführung 37, pp. 18–26.

Steam. (2021). *CS:GO - Overwatch System*. Retrieved from: https://help.steampowered.com/en/faqs/view/65DA-BD12-0DE9-9853. Accessed 21 November 2021.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research techniques*. Thousand oaks, CA: Sage publications.

Suchman, L. A. (1987). *Plans and situated actions: The problem of human-machine communication*. Cambridge, UK: Cambridge university press.

Taylor, T. L. (2003). Power gamers just want to have fun?: Instrumental playing a MMOG. *Proceedings of the 2003 DiGRA International Conference: Level Up (vol. 2).*

Tedlock, B. (1991). From participant observation to the observation of participation: The emergence of narrative ethnography. *Journal of Anthropological Research, 47*(1), 69–94. doi:10.1086/jar.47.1.3630581

Tichon, S. Makaresz, (2019). Influencing young adult social and personal identity through video-game narratives. *Asia Pacific Journal of Advanced Business and Social Studies, 5*(1), 116-129. doi: 10.25275/apjabssv5i1ss11.

Törhönen, M., Hassan, L., Sjöblom, M., & Hamari, J. (2019). Play, playbour or labour? The relationships between perception of occupational activity and outcomes among streamers and YouTubers. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*. URI: https://hdl.handle.net/10125/59694

Ubisoft (2022). *Reporting Cheaters FAQ*. Article number 000079704. Retrieved from: https://www.ubisoft.com/en-us/help/the-division/player-safety/article/reporting-a-player-in-the-division/000079704. Accessed 18 July 2022.

Van Maanen, J. (2011). *Tales from the field. On writing ethnography (2nd ed.)*. Chicago, IL: The University of Chicago Press.

Van Prooijen, J. W., & de Vries, R. E. (2016). Organizational conspiracy beliefs: Implications for leadership styles and employee outcomes. *Journal of business and psychology, 31*(4), 479-491. doi: 10.1007/s10869-015-9428-3

Vázquez, I. S., & Consalvo, M. (2015). Cheating in social network games. *New Media & Society*, *17*(6), 829-844. doi: 10.1177/1461444813516835

Vella, K., Klarkowski, M., Johnson, D., Hides, L., & Wyeth, P. (2016). The social context of video game play: Challenges and strategies. In Foth, M., Ju., W., Schroeter, R., & Viller, S. (Eds.), *Proceedings of the 2016 ACM Conference on Designing Interactive Systems (vol. 1)* (pp. 761-772). Association for Computing Machinery, United States of America. doi: 10.1145/2901790.2901823.

Voorhees, G. (2014). Chapter 31: Shooting. In Wolf, M. J., & Perron, B. (Eds.), *The Routledge companion to video game studies* (pp. 251-258). London: Routledge.

Walker, M. U. (2006). *Moral Repair: Reconstructing Moral Relations after Wrongdoing*. Cambridge: Cambridge University Press

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* (pp. 105-112). doi: 10.1145/1306813.1306839

Witschel, T., & Wressnegger, C. (2020). Aim low, shoot high: evading aimbot detectors by mimicking user behavior. In *Proceedings of the 13th European workshop on Systems Security* (pp. 19-24). doi: 10.1145/3380786.3391397

Wohn, D. Y., Jough, P., Eskander, P., Siri, J. S., Shimobayashi, M., & Desai, P. (2019). Understanding Digital Patronage: Why Do People Subscribe to Streamers on Twitch?. In *Proceedings of the Annual Symposium on Computer-Human Interaction in Play* (pp. 99-110). doi: 10.1145/3311350.3347160

Worrall, E-R. (2018). *Why are there no female pro players in Call of Duty?* Accessed 16 October 2021. Retrieved from: https://medium.com/@emilyokami/why-are-there-no-female-call-of-duty-pro-players-f229424999ab.

Wright, T., Boria, E., & Breidenbach, P. (2002). Creative player actions in FPS online video games: Playing Counter-Strike. *Game studies*, *2*(2), 103-123.

Wu, Y., & Chen, V. H. H. (2013). A social-cognitive approach to online game cheating. *Computers in Human Behavior*, *29*(6), 2557-2567. doi: 10.1016/j.chb.2013.06.032

Yan, J. J., & Choi, H. J. (2002). Security issues in online games. *The Electronic Library, 20*(2), 125-133. doi: 10.1108/02640470210424455

Yan, J., & Randell, B. (2005). A systematic classification of cheating in online games. In *Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games* (pp. 1-9). doi: 10.1145/1103599.1103606

Yu, S. Y., Hammerla, N., Yan, J., & Andras, P. (2012). A statistical aimbot detection method for online FPS games. In *The 2012 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-8). IEEE. doi: 10.1109/IJCNN.2012.6252489

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 & Entertainment, 37*(2), 513-551. Retrieved from http://www.cardozoaelj.com/wp-content/uploads/2019/06/YUN_NOTE-2.docx

Zonis, M., & Joseph, C. G. (1994). Conspiracy thinking in the Middle East. *Political Psychology, 15*, 443–459.

About the Authors

Arianna Boldi is a Ph.D. student in the Psychology Department at the University of Torino. Her research interests revolve around video games, self-tracking and intelligent agents, as well as the use of technology in the context of work.

Amon Rapp is an associate professor in the Computer Science Department at the University of Torino. His research interests revolve around self-tracking and wearable devices, video games, intelligent agents, and behavior change technologies.

List of tables

Table 1. List of data collection methods

Method	**Description**	**Target**	**Period of collection**
Observations	1) Participant observation of the gaming sessions played by the researcher and recorded 2) Observations of two tournaments (~12 hours long) played by streamers and broadcasted online	1) Amateur players belonging to the ethnographer's regiment or met randomly online 2) Streamers/players playing competitively	For the whole duration of the ethnography
Content of social networks and social media	1) 150 game-related posts and comments on Warzone Facebook groups 2) Contents (e.g., videos, posts) on 10 streamers' social media accounts (i.e., Instagram, Facebook, Twitter, Youtube, and Twitch)	1) Amateur players who joined Warzone Facebook groups (counting 107.602 members collectively) 2) The 10 most popular Italian Warzone streamers	For the whole duration of the ethnography
Informal conversations	Informal conversations with players on Warzone-related topics (about e.g., personal playing experiences)	Amateur players belonging to the ethnographer's regiment or met randomly online	For the whole duration of the ethnography
Semi-structured Interviews	Semi-structured interviews conducted online concerning the players' subjective account of cheating in Warzone	25 amateur players being part of the ethnographer's regiment or belonging to other regiments	Six months after the beginning of the ethnography
Ethnographer's diary	Field notes concerning the ethnographer's daily observations and reflections, relevant quotations gained from the informal conversations, interviews, relevant posts on social media and networks	The ethnographer herself	For the whole duration of the ethnography

Table 2. Categories of players and their characteristics

Category	**Hours spent in the game (avg.)**	**K/D ratio (avg.)**	**Matches played (avg.)**
Master	1273	1,48	4652
Average	250	0,75	1145
Novice	112	0,49	400

Table 3. Sample

ID	Age	Genre	Education	COD	Battle Royale	Warzone expertise	Platform	Role
P01	23	M	High school	Yes	No	novice	Console	Member
P02	38	M	Middle school	No	No	average	Console	Member
P03	32	F	High school	Yes	No	average	Console	Member
P04	23	M	Middle school	No	No	average	Console	Member
P05	24	M	Bachelor's degree	Yes	Yes	average	PC	Member
P06	25	M	High school	Yes	Yes	master	PC	Founder
P07	33	M	High school	Yes	Yes	master	PC	Member
P08	40	M	High school	No	Yes	novice	Console	Member
P09	42	M	High school	Yes	Yes	novice	PC	Member
P10	24	M	Middle school	No	Yes	master	PC	Member
P11	52	M	High school	No	Yes	novice	Console	Member
P12	34	M	High school	Yes	Yes	novice	PC	Member
P13	37	M	High school	Yes	No	average	Console	Member
P14	30	M	Middle school	Yes	No	average	Console	Member
P15	31	M	High school	Yes	No	novice	Console	Officer
P16	30	M	High school	Yes	Yes	master	Console	Officer
P17	34	F	Master's degree	Yes	No	novice	PC	Officer
P18	30	M	Master's degree	Yes	No	novice	PC	Member
P19	25	M	Bachelor's degree	Yes	No	average	Console	Officer
P20	31	M	Master's degree	Yes	No	average	Console	Officer
P21	22	M	High school	Yes	No	novice	PC	Member
P22	42	M	High school	Yes	Yes	average	Console	ND
P23	24	F	Bachelor's degree	Yes	Yes	novice	Console	Officer
P24	24	F	Middle school	Yes	No	average	Console	Member
P25	41	M	Master’s degree	Yes	No	average	PC	Officer

Table 4 – Key findings

Cheating in Warzone from the participants' point of view	
Who the cheaters are and what cheats are	Knowledge of cheating
- Participants attribute the label "cheating" to different in-game behaviors depending on who performs the cheating behavior and the "role" she has in the game community - Technology equipment may be considered a cheat even if it is "legal" and there is a grey area that may be characterized as cheating or not by different players	- Participants have fragmented and incomplete knowledge of all the cheats that are currently available in the game - Knowledge around cheating is often the result of word-of-mouth, also due to the technological sophistication of cheats - The vagueness of knowledge makes cheating an uncertain phenomenon
The role of competence	
Novice and average players	Masters and streamers
- Novices ad average players have few criteria to recognize cheaters and are often prey to rumors and "sensations" in making their judgments about cheating - They do not have the competence to exploit the technological aids made available by the designers to analyze the in-game actions and discover unfair behaviors	- Master players have competence to identify those behavior that may be unfair: to do so, they utilize a variety of strategies like comparing the potential cheater with a "model" of the player and using statistics and metrics - Likewise, streamers have the competence to detect cheating, which allows for an in-depth analysis of the technological features of the cheats
The consequences of cheating	
Paranoia	Surveillance culture
- The uncertain nature of cheating encourages the spreading of "conspiracy theories" and contributes to creating a climate of paranoia, where every player may be accused of cheating. - Reciprocal accusations of cheating may be a way to rework negative feelings coming from a defeat, but they may fuel the climate of paranoia	- For amateurs, observing the other may be a means to regain agency and sense of control over cheaters, while for streamers it may be a way to show that they are the "paladins" of the community - Reciprocal observation is sustained by the design features of the game - Total transparency and the climate of "paranoia" may culminate in a sort of surveillance culture, where each player and streamer observe and are observed by others