The Slippery Slope: Exploring the Parallels Between Game Cheating and Cybercrime Through Routine Activity Theory

Selina Cho
Dept. of Computer Science
University of Oxford
Oxford, UK
selina.cho@cs.ox.ac.uk

Jonathan Lusthaus
Dept. of Sociology
University of Oxford
Oxford, UK
jonathan.lusthaus@sociology.ox.ac.uk

Ivan Flechais
Dept. of Computer Science
University of Oxford
Oxford, UK
ivan.flechais@cs.ox.ac.uk

***Abstract*—Law enforcement agencies have expressed concerns about the potential connection between video game cheating and engagement in cybercriminal activities among young users. This study conducts a preliminary investigation into this topic by examining the parallels between game cheating and cybercrime, using Routine Activity Theory (RAT) from the field of criminology. Through a systematic analysis of previous empirical studies and an extensive review of relevant literature, the findings uncover previously overlooked themes between the two domains: a drive for victory, exploiting user and system integrity, attack-defence dynamic, social immersion and domain familiarisation, and anonymity. The study then provides a discussion on steering users towards pro-social practices in the cyber security industry, while also addressing the potential unintended exposure of users to cybercrime. The outcomes of this research underscore the need for continued enquiry by researchers and policymakers to gain a more nuanced and comprehensive understanding of the potential link between game cheating and cybercrime. The study concludes by offering reflections on its limitations and the applicability of RAT beyond its traditional context.**

***Index Terms*—routine activity theory, video games, cheating, cybercrime, cyber security**

I. Introduction

In recent years, law enforcement has started probing the underlying factors associated with cybercrime to develop early intervention strategies that seek to deter novices from offending. Cheating and unauthorised modding in video games are areas of particular interest, commonly considered as avenues through which young individuals might transition towards cybercrime. In 2017, the UK National Crime Agency (NCA) claimed that cheating or modifying games serves as a "slippery slope" for adolescents [1], pointing to forums exposing them to malware and like-minded enthusiasts who also engage in cybercrime. A similar report by NCA's National Cyber Crime Unit maps the gradual stages of progression which some youth players experience before fully engaging in illegal activities online [2], urging the need to better understand the nature of the elements bridging the two domains.

Despite some evidence highlighting the potential association between cybercrime and online games [3], [4], the actual interplay between game cheating and cybercrime remains underexplored in academia. Game cheating often involves manipulating the code and memory of online games, giving players an unfair advantage [5], [6]. Players without the technical expertise to do this themselves are attracted to online forums, which provide convenient access to pre-made cheat tools [4], [7], some of which have been known to contain malware [8]. As such, both academic and industry observations have pinpointed some elements of game cheating that resonate with core principles of cyber security [5]. However, the current observations do not sufficiently establish a definitive 'pathway' from one activity to the other [1]. In fact, making surface-level associations with cybercrime can perpetuate a generalised perception, categorising all cheating players as potential cybercriminals. This overlooks broader social ramifications and the potential insights which may be beneficial for the cyber security industry. As a result, a more nuanced analysis and a thoughtful approach are needed to discern the parallels between these two domains before determining any direct progression between them.

In this research, we delve into the potential parallels between game cheating and cybercrime by employing Routine Activity Theory (RAT) [9]. This widely cited criminological theory offers a robust blueprint for researchers to understand the patterns surrounding a variety of transgressive or criminal scenarios. We first apply RAT to game cheating, and then highlight the parallels and differences with cybercrime. We distinctly emphasise the term *parallels* over *similarities*: while *similarities* often refer to the technical and surface-level resemblances between two entities, *parallels* go deeper, encompassing the intrinsic patterns or trajectories that the two might share. This distinction enables us to examine how two activities can have comparable traits or patterns across varied settings without necessarily being functionally equivalent or

This research was funded in part by Engineering and Physical Sciences Research Council [EP/P00881X/1].

converging into a singular pathway.

The following sections comprise this paper: 1) We provide a brief background on game cheating; 2) We outline the core elements of RAT; 3) The methodology section chiefly engages with two elements, involving a) a secondary analysis of the data collected during our earlier empirical studies on game cheating (detailed in Section IV), and b) a systematic literature review of the perspectives on cheating; 4) We apply RAT to game cheating; 5) Parallels are drawn with cybercrime; 6) We offer discussion regarding broader points on cyber security and the limitations of this study.

II. Game Cheating and Security

In the context of online gaming, cheating is the act of gaining an unfair advantage over an opponent against the rules, as enforced by the game operator [5]. Cheating is a broad term that varies across cultures and contexts [10], [11]. In 2005, Yan and Randell provided a foundational taxonomy of online game cheating [5], raising the need to factor in security perspectives in protecting the integrity of games. They argue that the traditional principles of security (e.g., confidentiality, integrity, availability, and authenticity) cannot explain the security failures highlighted by cheating. They also contend that no matter what forms of security issues arise in games, it is ultimately the value of fairness and its enforcement which guide the role of security in game-specific applications. Unlike offline games, where players can be monitored in person, online games necessitate dependence on technical security capabilities to enforce fairness.

Despite the semblance of security-minded skills required to cheat, a new trend has risen wherein the cheating players themselves started to fall prey to cyber attacks and fraud. Publisher of the Call of Duty series, Activision, released their 2021 report [8] on fraudulent cheats, which rely on persuasive advertisements to trick players, especially novices, into installing malicious software. Under the guise of installing a legitimate cheat tool, these scams lure players into voluntarily lowering their security settings to gain a more seamless cheating experience, when in fact, it is bypassing the protections for deceptive purposes. The threat statistics recently obtained from security companies also point to a myriad of game-related cyber threats victimising users both within and beyond the gaming environments [12], [13].

The most intuitive threat faced by the players who cheat is the anti-cheating teams of game companies. In the vast majority of online multiplayer games today, when a player is caught cheating in an online game, they are banned from accessing the game again, either temporarily or permanently. Due to the negative impacts of cheating, especially on multi-player games, game publishers have invested heavily in anti-cheating teams, dedicated to the prevention, detection, and elimination of cheating from their game platforms. Given the relevance of technical security in the mechanics of cheating [8], game companies often collaborate with security companies to bolster their anti-cheating efforts. Some security experts take an outside-in approach, starting with general security attacks of relevance (e.g., Sophos and Kaspersky [12]), then investigating cheating communities that seriously display these malicious endeavours [4], [7]. The dynamic between cheating players and anti-cheating teams resembles the classic cat-and-mouse game seen in the broader cyber security industry.

III. Routine Activity Theory

Developed by Cohen and Felson, Routine Activity Theory (RAT) [9] posits that a crime will occur if a motivated offender deems a target to be suitable and a guardian absent (Fig. 1). Widely applied across a variety of criminal behaviours offline, RAT provides a situational assessment of crime from the perspective of an offender, prompting ideas for prevention strategies.

Fig. 1. A visual representation of Routine Activity Theory.

In 2005, Yar [14] examined the applicability of RAT for explaining the patterns of cybercrime, and discussed its applicability to online mediums, with regard to spatiality, temporality, and the conversion of the physical guardians to an online equivalent. Some scholars [15] point to instances where components can be scoped down further to correspond to the RAT elements (e.g., anti-virus software as an equivalent of a guardian, and overexposure through the routine online activity as a description of a suitable target).

Since then, an increasing number of studies have used RAT to describe specific types of cybercrime (e.g., virus, malware, phishing, fraud, and cyberstalking [15]–[18]) [19]. Transposing the core elements of RAT reveals a high degree of variation within cybercrime. For instance, motivated offenders are seen in examples of hackers, scammers, and stalkers, while targets may be proprietary data, sensitive information, payment details, or the computer infrastructures which support these assets. The guardians, or lack thereof, may be private companies, law enforcement, or any entity that opposes the potential offender. Moreover, not all elements of RAT are equally significant in explaining cybercrime [19]. Leukfeldt and Yar expand on Yar's initial work [14] by determining the usefulness of the theory in explaining different types of cybercrime with a focus on victimisation [19].

A. RAT in the Context of Cyber-Dependent Crime

Cyber-dependent crimes offer the closest point of comparison to game cheating. This subset of cybercrime targets computer systems and networks, through hacking, malware and

other forms of unauthorised intrusion [20]. Researchers have identified that motivations for participating in cyber-dependent crimes include financial gains, the satisfaction of overcoming technical challenges, ideological beliefs, and the attraction of online anonymity [21]–[24]. Regarding the absence of guardianship, it frequently refers to technical measures like antivirus software but it also includes personal guardianship, which relates to a potential victim's awareness and capability to defend against such threats [19], [23]. Suitable targets are typically characterised by their prominent visibility (e.g., frequenting specific websites) and accessibility (i.e., the ability for others to reach them either directly or indirectly). Notably, targets associated with substantial financial rewards are attractive, especially in the context of malware [19].

IV. Methodology

There are two core elements of our data and methods. First, we carried out a secondary analysis [25] of the empirical data collected from our prior studies. Second, we carried out a systematic literature review of empirical research published in the past 20 years. The two datasets were initially analysed separately using thematic analysis, which was informed by the RAT framework, and then analysed side-by-side to scope down to the most prominent themes. The identified themes were subsequently examined for the intersections they share with the cybercrime application of RAT.

As noted, this study defines game cheating as activities that are not authorised by game developers. Our approach spans various game genres, acknowledging that the nature of unauthorised behaviours, including cheating, hacking, modding, and glitching, varies by context. The terms 'modding' and 'cheating' here denote unauthorised actions. In the context of *GTA V Online*, 'modding' is specifically used to describe unauthorised modifications that adversely affect other players, as opposed to actions that are positively endorsed by the game developers.

A. Data Collection

1) Dataset 1 - Secondary Analysis: Secondary analysis involves the use of existing data which was originally collected for a prior study to contextualise it to a new research interest [25], [26]. It is a widely used methodology in qualitative research as it allows researchers to extract "further analysis of an existing data set which presents interpretations, conclusions, or knowledge additional to, or different from, those presented in the report on the inquiry" [27].

We started the secondary analysis by reviewing the data collected from our previous studies on game cheating which broadly consisted of two topics: the user experience of cheating (study B: [28]) and the governance of cheating communities (study A: [29], [30]). The decision to revisit the existing dataset arrived during the analysis process of study A, where the authors observed concepts associated with cyber security. The two studies consisted of online interviews with participants with experience in cheating. The interviews were semi-structured to allow for open-ended responses, which could organically bring in participants' beliefs and feelings about cheating.

We started with purposive sampling, using advertisements posted on cheating-related forums in Reddit, between October 2020 and July 2022, with approval from forum moderators. When potential participants indicated interest, we asked for their preferred mode of platform for being interviewed. As the interviews continued, we adopted snowball sampling through recommendations and direct messages to those interested. The inclusion criteria for participation were to 1) be either 18 or over, 2) have experience engaging with the corresponding cheat community within the past ten years, and 3) speak English. The interviews lasted between 25-50 minutes, and were either carried out via text or audio (which were transcribed afterwards). The studies were carried out with institutional ethical approval (ref no.: SSD/CUREC1A CS_C1A_20_017). The interviews in study A were designed to inquire about the foundations of community governance in game cheating from an exploratory perspective, while B focused on the aspects of player experience in cheating. It is worth noting that the latter study took an exclusively play-centric approach to the topic, distinct from most research that positions cheating as something to deter. The interview protocol is presented in the Appendix. Aside from the interview data, the researcher also took notes, including the participant's impressions and descriptions of the visual contents (e.g., gifs or brief screenshares by the participant) that were observed during the interviews.

2) Dataset 2 - Systematic Literature Review: Systematic literature review (SLR) is concerned with aggregating empirical evidence to support an evidence-based paradigm [31]. It is obtained through various techniques, often with different scope and contexts but has proven useful for systematically assessing and guiding researchers to objective summaries of empirical data. The nature of the second dataset differs from the first in that we focus on synthesising evidence that arose from primary studies, instead of re-analysing the original dataset [32]. In earlier works exploring comparative textual analysis of published work, Noblit and Hare [33] discuss how interpretive literature reviews can achieve synthesis by involving the concepts which already surfaced in the original studies into a "higher-order theoretical structure" [32]. More importantly, SLR helps establish a criterion on which to evaluate the validity and quality of a work, by potentially revealing inconsistencies or contradictions [34]. Thus, to validate and extend our findings from dataset one, we carried out SLR on the existing literature on game cheating.

We reviewed major literature known for its influence in industry or academia in the past 20 years, which is when scholarship in online game cheating started to become more common. We used Google Scholar and ACM Digital Library to search the articles using keyword phrases ("game cheating", "cheating behaviour", "multiplayer games"). We also reviewed the references and citations of seminal works of scholars dedicated to cheating [6], [35], [36] to locate other relevant work. The inclusion criteria were that the literature

is a qualitative empirical enquiry exclusively into cheating in multiplayer games, is published in a peer-reviewed venue, and it concerns the user perspectives of those who cheat.

The sampling was purposive, rather than exhaustive. Thus, the search was stopped when we reached a theoretical saturation [37]. The list of literature was compiled with the following elements: title, authors, date, abstract, the abstract, and publication venue. Our preliminary list of the dataset included 42 research articles, industry reports, and news articles in the field of HCI, game studies, and cyber security. We comprehensively reviewed the contents of the literature three times in total, with a focus on the RAT elements, taking notes of the summaries, notable arguments, and findings. The quality of the chosen studies was assessed according to their appropriateness and quality of the reporting (e.g., how detailed and rigorous are the aims, context, and methods of the study) [38]. Items which did not meet the assessment criteria or the inclusion criteria were removed. At the end of the iteration, we had 12 items remaining for analysis.

B. Data Analysis

The methodology we utilised for the secondary analysis was thematic analysis [39]. Thematic analysis is commonly used in qualitative research to identify themes, or patterns or meanings in the data which can be used to provide more insights into an issue or a research topic. While the process of thematic analysis involves the development of categories and classifications to describe the data, the analysis itself goes further in depth to enrich it with interpretations and insights. The themes incorporated in RAT encompass both semantic (explicit meanings or what the participant has said [40]) and latent (underlying meanings or assumptions) themes. The significance of a theme is not necessarily representative of its frequency of appearance in the data.

The purpose of using the thematic analysis method is to uncover deeper meanings embedded in the interviews that went beyond identifying universal facts. It is also procedurally relevant to other methods of qualitative research, which rely on coding and searching data sets for themes in the process. The first author led the research for prior studies on game cheating [28], [29], which were analysed using grounded theory and content analysis. These analyses took an inductive approach, wherein the themes were purely derived from the data [39], [40]. However, for the analyses of the two datasets in this study, we took a deductive approach using RAT as a pre-existing theory to identify the themes of interest for the new research focus.

1) Dataset 1: Thematic Analysis: The thematic analysis of dataset 1 followed Braun and Clarke's 6-step method [40].

1. Familiarising with the data: The first author began by familiarising themselves with the entirety of the data, including the notes and text descriptions of participant-side screenshares. Even though the data had previously been thoroughly observed, this foundational step allowed the author to gain a renewed orientation of the data [41] in the broader context of cheating, rather than specific to a certain game.

2. Generating initial codes: The author took notes on items of interest, relevant questions, and connections between the observed data. The codes were chosen so that they do not overlap while fitting in a larger coding manual. The author took note of the developing order of the codes to keep track of the author's interpretations in the latter part of the analysis. Once the first round of coding was done, the author applied the codes back to the data to find overlapping themes or connections. Coding was carried out on NVivo software.

3. Searching for themes: The first author then examined the codes together with the two co-authors to find broader themes. This step involved analysing, comparing, and visually mapping the codes to draw relations and relative significance [42]. Following a deductive approach, our analysis was informed by the existing concepts and limitations in RAT literature [9], [19].

4-5. Reviewing, defining, and naming themes: This step involved reviewing the data within the themes to ensure they have adequate coherence and commonality [41]. The thematic labels were revised to better reflect the data and clarity.

6. Producing the report: The final step involved recording the findings, with a descriptive account of how the researchers interpreted the observed data and themes. These descriptions form a part of the subsequent section discussing cheating in the context of RAT.

2) Dataset 2: Thematic Synthesis: Thematic analysis in the context of a systematic literature review (also referred to as *thematic synthesis*) provides a clear identification and structure of prominent themes. Although sharing many similarities with thematic analysis of primary data, thematic synthesis requires a few additional considerations. Dixon-Woods et al. [32] emphasise the importance of distinguishing between the thematic synthesis that is driven by the themes within the literature, or driven by theory, which is centred around evaluating specific themes by engaging with the literature, for purposes of transparency. Our approach was theory-driven in that it explored the literature with a particular focus on the RAT elements, iteratively going back and forth to see how and whether they relate to one another.

We followed the three-stage synthesis protocol from Thomas and Harden [43]. The first two steps involved coding the text of the literature, and developing preliminary descriptive themes. The third step aimed to go beyond the findings of the primary studies by generating additional concepts and open-ended questions. As part of this process, we replicated the step 4-5 in Braun and Clarke's 6-step method [40], and finally synthesised the parent themes.

3) Final Integration and Synthesis: Upon finalising the analysis process with dataset two, we compared the themes side-by-side with those surfaced in dataset one to categorise them into the most comprehensive units. Through iterative coding of the themes, we settled on a parent branch of the themes encompassing the minor ones.

C. Sample Overview of Dataset 1 (Interview participants)

The study involved interviews with 70 participants (A: 43, B: 27) experienced in video game cheating, including both former and current cheaters. This also included individuals in roles that facilitate the act of cheating, though they may not engage in it themselves. This includes former and current moderators responsible for overseeing online communities (n=19), cheat developers who specialise in creating and testing cheat software (n=14), and content creators who produce a variety of media for digital platforms (n=11). Despite the inherent differences in these roles, a common factor is that many participants also engage in playing the games themselves. We recognise the nuances involved in these different roles within our study, and address this in the Discussion section.

Although the interviews were in English, the participants were based in over 21 countries, with the two largest proportions coming from the USA and the UK. To ensure anonymity, the profiles of the participants were not, and could not be, screened prior to the interview. However, 84% (59) of the participants self-identified as male, while one was non-binary and the rest either did not identify or chose not to respond. Sixty percent of the participants were below the age of 21 with the oldest being 32 and the youngest 18.

Spanning multiple genres, the games that were discussed[1] during the interviews include *Counter-Strike: Global Offensive (CS:GO)* (43), *Grand Theft Auto V Online (GTA V Online)* (24), *World of Warcraft* (1), *Dota 2* (1), and *Dark Souls* (1). As observed, there was a high discrepancy in the response rate across different cheat communities which is likely reflective of the differences in the size of the userbase or average user activeness. *CS:GO* had the largest userbase of all the cheat communities we posted the advertisements on.

V. Applying the Routine Activity Theory

The following describes the key themes we identified in relation to cheating, according to the three elements set out by RAT: a motivated cheater, lack of guardians, and suitable targets. Here, we use randomised pseudonyms which have no real-life association with any participant's identity.

A. A Motivated Cheater

Advancement. There are various reasons why players choose to cheat, and the advancement aspect is the strongest (supported byboth our data analysis and prior studies). Players wish to gain victory without investing as much time or energy into playing games. They resort to cheating or external help when they run into roadblocks in a game to get past the point of difficulty, regardless of whether they recognise it as a form of cheating or not. Cheating also allows them to skip to new or unexplored sessions more quickly. For those who are bored of playing the same format of a game, cheating introduces a new form of positive experience. According to Consalvo [6], it helps enable players to "salvage some fun out of the game" as they would not wish to continue playing otherwise.

Cheating also allows players to progress and move through the ranks quicker than they otherwise would. A player can even adopt a more superior 'god' mode to control and oversee others in a multiplayer game. This is not only more convenient in progressing faster but some players simply enjoy the satisfaction they gain through it as they appear to be better skilled than they actually are.

Curiosity. When bored or frustrated with the standard gameplay, players may become curious and begin to set new objectives within the game [6]. Notably, cheaters perceive the act of finding the flaws and vulnerabilities in the game system to be a new form of a game-within-a-game, or a meta-game, in itself. Consalvo [6] found from her interviews that some players often perceive themselves as "elite" players who have gone beyond the average level of challenges generally offered by the game, and thus seek to "gam[e] the game" itself by discovering glitches and exploits. For a player unsatisfied with the original layout of a game, this offers opportunities to rehash existing elements for refreshed, enjoyable experiences, keeping their interest anchored to the game. In such cases, ethical dilemmas related to cheating become secondary in light of the sheer enjoyment it provides. Moreover, their desire to cheat is not primarily driven by an intention to harm others but more for self-serving purposes; they primarily aim to fulfil their purpose of playing games, which is fundamentally to have fun. However, there are still cases when some cheaters intentionally cause harm or disruption in games by trolling or flaming: according to Paul from Reddit's *CS:GO* cheating community, "toxicity is allowed, as long as it's taken with a pinch of salt or has any humour factors behind it".

Cheaters aim to discreetly yet continuously outpace the game publishers in the ongoing tug-of-war between cheating and anti-cheating measures. Over time, this determination can lead them to devise novel and unconventional cheating methods. One of the participants, Alex explains "the war between anti-cheat and cheaters is the same age old battle. Bullets vs bulletproof vests. Tanks vs armor piercing rounds. Better cheat detection vs better cheats. One side makes an improvement and the ball is back in the others court to outdo the other". Brian also adds: "The better the ac [*anti-cheat*] just means the better the cheaters".

Resentment. Over time, accumulated negative feelings and experiences can intensify one's desire to cheat or, if pushed further, deter them from playing the game altogether. Matt with experience in *CS:GO* explains, "the thing is valve, (the company that runs counter strike) does not care about its own game, only about the money it generates. they dont do anything with their anticheat they just want people to be banned so they buy accounts again". Players come together in games seeking a 'good' gaming experience—i.e., one that is engaging and enjoyable. Yet, when the expected quality falls short, they may feel that game developers are not as invested in enhancing the game. Dan expresses "I cheat on the game to say 'look

[1]The versions of the games are removed to minimise redundancy, especially as some participants had experience playing more than one version in a given game series.

the game would be good - just fix it'. That's why I look for exploits because if I can find a game-breaking exploit, that can really ruin the game, then I can just keep using it over and over until they are forced to fix[] the game".

Anonymity. With prolonged exposure to successful episodes of cheating, cheaters can absorb the norms and rules of the cheating community. With the ability to shield their real-world identities through online platforms, cheaters undergo a rationalising process for their act of cheating to establish new meanings and acceptable forms of behaviour [36]. The shield provides a layer of safety to the user such that their cheating activities are less likely to be tied to their real-world persona: "Sometimes, i don't like to play with my own name of csgo cheating servers, because if i do, people would recognize me and trashtalk" (Sam). This can sometimes result in cognitive dissonance, whereby a cheater may be frowned upon for breaking the rules in the general gaming context but in a community of pseudonymous cheaters, they are actually highly respected within a different system of norms. A notable observation from the first dataset highlights this dynamic: while reverse engineering is a common practice, using it on cheat software created by a respected member is often strongly frowned upon. In fact, engaging in such an act can result in significant repercussions, including the possibility of being banned from private forums or ostracised by peer groups. As such, individuals in these communities adopt pseudonymous identities that align with the evolving norms and practices, while keeping their real-world identities concealed. Furthermore, an individual's standing within the community often determines the extent to which they can contribute to shaping its norms and practices [30].

B. Lack of Guardians

Limited anti-cheating capacities or efforts. Guardianship in the online context can be recognised in both technical and social terms [19]. From the perspective of a potential offender, the gravity of the threat posed by the anti-cheat teams—by their size, sophistication, or the severity of the punishment they can deliver—is an important consideration. However, when a game publisher lacks the resources to invest in a dedicated anti-cheating team, its game products may suffer from cheating attempts by players who see an opening. Even established anti-cheating teams may be under-resourced or over-worked, or may not be fully motivated, or not perceive cheating as a major concern [44].

There are reasons why game companies may not seek to be aggressive guardians against cheating. One participant who frequently mods in *GTA V* explained: "GTA V online is a sandbox that has a lot of restrictions applied in order for Rockstar to monetize the game. Rockstar doesn't have much of an incentive to make actual good new content because people keep buying the game and shark cards anyway. Modding the game allows you to add your own features/content without having to rely on Rockstar to do it. This gives the game near endless replay value". Subscription-based games depend on the players' willingness to keep paying. According to Alex who has experience playing massively multiplayer online role-playing games like World of Warcraft, "each botter is [] someone paying $15 to play the game. So Blizzard doesnt have a HUGE incentive to permanently ban these people, especially as they continue to have a dwindling population". Therefore, even if a player cheats, they objectively remain a contributing member to the overall userbase. In this case, banning a cheater outright from the platform may not be the most attractive option for the publisher.

Limited interference by legal authorities. Arrests and legal threats arising from cheating are perceived to be rare. There are several possible reasons for this. Primarily, the average player often lacks clarity on the specific laws breached during certain activities, making it unlikely for them to recognise and report. John who has been cheating in *CS:GO* for years claims that "you can gain [an] advantage [the] dirty way without getting caught by police" which is what makes it "satisf[ying]". The practice might also be deemed relatively minor and thus not worthy of the attention of the police. Further, the fleeting nature of game-related interactions makes it challenging to report in a timely manner unless it has been recorded elsewhere. Chris shared his recent experience using his tool in *GTA V Online*: "[I have] never been killed with it active. People try to, then get mad and report me, so my menu detects it and crashes their game and cancels the report".

Jack, who has significant experience overseeing cheat companies and projects, underscored a strong focus placed on legal considerations: "As video game cheats exist in sort of a grey market, there are a lot of things to keep in consideration for running a proper company. Copyright infringement is the main legal issue with video game cheats, so maintaining an air of plausible deniability or side stepping the laws around it is needed". Outside of any game company guardianship, the blurred boundaries are largely left to the player to resolve, who decides what cheating-related behaviour can be carried out and when. This indicates that, even with increasing attention from law enforcement, there remains a lack of attention in this particular area, compounded by ambiguous understandings of which activities are considered illegal. It should be noted that our data primarily focuses on aspects related to cheating in games and, as a result, does not encompass the scope of law enforcement interventions in activities associated with, but external to, gaming, such as DDoS-for-hire services.

C. Suitable Targets

'Well-designed' games. One interesting perspective that surfaced is that games with some form of rewards at stake—whether actual in-game rewards or merely having a positive experience—are attractive to cheaters. While this is common knowledge in general gaming, it is interesting that the same holds true for individuals specifically interested in cheating. Alex explains that the fun derived from cheating is essentially no different to that derived from playing by the rules: "the very mechanics in games that encourage cheating, are also there to reward players who do the long grind. Any game that isnt worth cheating in, probably isnt worth playing", and adds

"you know how you stop cheaters? You make a shit game", suggesting that cheaters are motivated to take up a challenge when the target subject appears valuable. This could imply that large game franchises with active maintenance by the game companies or considerable commitment to in-game values will attract more cheaters than other games without such elements.

In-game opponents. In synchronous multiplayer games, the presence of other players can increase competitiveness and thus the desire to gain victory over one another through unauthorised means. Brian described that cheating "let's [him] be competitive and actually need to try to win but at a higher level than [he]'d usually be able to". As such, multiplayer games may be more suitable targets for cheaters than single-player games. David shared: "one friend in particular was extremely competitive, and would just be very mad if he didn't win, and that kind of stuck with me a bit. [...] I never cared about winning until my friends made me care about it, and cheating makes me not die for stupid reasons". In some ways, the acts of cheating may be more accurately directed towards opposing players rather than the game itself.

Vulnerable systems. Game infrastructures are vulnerable to exploitation due to their role in deploying services. This vulnerability attracts cheaters, and represents a key factor in identifying suitable targets within RAT. A cheater may tamper with the servers or change the configurations once they have access to the central host systems. Some can modify their client end of the system infrastructure, or exploit a flaw in the operating system or network protocols to break into the server side. Dan points out, "I can show you free exploits which shouldn't exist in the first place if the developers just knew what they were doing". One can also cheat by abusing the operational procedure of a game, without a significant level of technical sophistication. In short, games with vulnerable systems present suitable targets for exploitation.

VI. Uncovering the Parallels between Game Cheating and Cybercrime

Following the application of the RAT schema, we are able to highlight the parallels between game cheating and cybercrime. First, the RAT themes relevant to both cheating and cybercrime are presented in Table I. Their shared elements were re-labelled to appropriately represent the context within both domains, as highlighted in Table II. Curiosity is encapsulated in *Victory & Advancement* as they represent the desire to learn and progress forward in games. *Integrity & Fairness* is linked to the notion of personal guardians, wherein individuals or systems may lack the awareness to defend themselves. *Attack-Defence Dynamic* represent the role of technical guardians, where the technical resources determine the quality of the interaction between the offensive and defensive responses. We categorise *social Immersion & Domain Familiarisation* under accessibility because having access to the relevant social network and domain knowledge empowers users with the appropriate information regarding suitable targets and methods for cheating.

TABLE I
Routine Activity Theory Themes within Cheating and Cybercrime.

	Motivated cheater	Lack of guardians	Suitable targets
Cheating	Advancement Curiosity Resentment	Anti-cheating Legal authority	In-game opponents Vulnerable systems Well-designed games
Shared themes	Anonymity Curiosity	Technical guardians Personal guardians	Accessibility
Cybercrime	Financial gains Ideological beliefs		High visibility High-income user

TABLE II
Resulting themes, along with the corroborating references.

Reference	Victory & Advancement	Integrity & Fairness	Attack-Defence Dynamic	Social Immersion & Domain Familiarisation	Anonymity
Consalvo [6]	✓		✓	✓	
Mortensen et al. [45]		✓	✓		
Meades [46]	✓	✓	✓		
Wang et al. [47]	✓	✓	✓		
Fields & Kafai [48]				✓	
Irwin & Naweed [49]	✓	✓		✓	
Dumitrica [50]	✓		✓	✓	
Chen & Wu [51]				✓	✓
Boldi & Rapp [52]	✓	✓		✓	
De Paoli & Kerr [53]	✓		✓	✓	
Wu, Hu & Li [54]		✓			✓
Chen & Ong [36]	✓	✓		✓	✓
Study A [29], [30], [55]	✓		✓	✓	✓
Study B [28], [56]	✓	✓	✓	✓	

A. Parallels

1) The Pursuit of Victory and Advancement: In both game cheating and cybercrime, violators commonly rationalise deviating from set standards to reach their objectives. At a glance, most common motivations for cheating (e.g., gaining victory and expediting progress) are primarily contextualised within the gaming environment, underpinned by the notion that players must meet specific benchmarks to win [57]. Lindley, a game researcher, posits that obedience to rules only suggests a particular style of gameplay, not necessarily resulting in a fulfilling gaming experience [58]. He suggests mastering a game involves grasping its interaction patterns, some of which may veer outside the official rules. Techniques such as ninja looting[2] exemplify this. In such scenarios, players might strategically skirt around accepted rules and norms if it draws them closer to their objectives.

[2]Ninja looting is when a player unfairly acquires loot from a defeated opponent. This looting offers an easier entry point to secure these items.

Cybercriminals share a victory-oriented mindset focused on achieving their objectives. For example, a cybercriminal driven by financial gains will deploy malware specifically designed to exploit vulnerabilities in online payment systems [59]. Some publicly showcase their earnings through partying or purchasing expensive cars [21]. Others brag online. Outside of profit-driven cybercrime, this victory mindset is also apparent. It is well-known that individuals involved in various forms of hacking, such as website defacements, publicly report and discuss their deeds as part of attempts to increase their standing within online communities [60], [61].

2) Exploiting the Integrity of Users and Systems: Both cheating in games and cybercrime rely heavily on the consistency and predictability of users and systems for effective exploitation. In gaming, there is a prevailing assumption that players will conform to set rules, with game systems and infrastructures operating reliably to uphold the gaming environment. In such settings, deviations (e.g., exploiting a game glitch or a network lag, or using modified game clients) challenge the foundational premise of integrity and fairness [5], [62]. In gaming environments, where fairness is critical to maintaining the game's intended trajectory, cheaters can manipulate this by exploiting other players' commitment to the rules. This situation speaks to the concept of personal guardianship within RAT, where some players are inadequately equipped to defend against exploitation.

In a similar way, cybercriminals operate on the assumption that targeted systems and users will operate according to predictable patterns, forming the basis for offenders to initiate attacks. The work of Lusthaus and co-authors finds that cybercriminal business models are surprisingly stable and that offenders from malware networks across fraud networks continue to use tactics that have been shown to work. They are reluctant to change their approaches, unless the patterns of the users and systems they target change [59], [63]. As such, the common thread between the two communities is the exploitation of anticipated behaviours and vulnerabilities.

3) The Attack-Defence Dynamic—Procedures of Deployment: The technical configurations of some game cheats often mirror hacking methodologies and the principles of malicious software deployment [4], [7], [8], [13]. Many modern online games operate on client-server architectures, managing myriad tasks essential for a seamless gaming experience. But this design also offers avenues to cheat. Players, on the client side, can access and alter game files or graphic drivers, changing in-game values such as player resources. Using memory editors, the cheats can bypass traditional file-based detection. Memory editing tools function by accessing and modifying the values stored in a game's active memory space, resembling how certain malware manipulate memory to inject malicious code or read sensitive data. Other cheat tools may also employ techniques such as API hooking to alter the behaviour of the game software, which is a common method used by malware to intercept and modify system or application calls. An experienced cheat developer, Tim explains: "Anticheats have advanced a lot in recent years and I believe the AC / Cheater industry is about 5 years more advanced than the general infosec community. The cat and mouse game has moved from simple memory cheats, to Hypervisor systems and virtualized drivers".

Anti-cheating teams respond to such cheating attempts by enhancing their defence strategies, reflecting the common reactive stance observed in general security operation centres. These elements fall within the guardianship component of RAT. Although, as noted above, if systems are left vulnerable, they become suitable targets, and are also relevant to that RAT component. Beyond the technical realm, the attack and defence dynamics involve key actors within groups whose presence not only facilitates but also significantly increases the likelihood of a successful attack. This aspect is highlighted in previous studies on cybercrime groups, such as those by Biswas et al. [64], which discuss the influential roles the actors play in executing operational activities. Hughes et al. [65] apply the focus of key actor identification, as explored in earlier hacking forum research by Pastrana et al. [66], to the specialised domain of game cheating forums.

4) Social Immersion and Familiarisation with Domain Knowledge: The social dynamics of the cheating community provide insights into how some players become familiar with concepts often associated with cybercrime, without necessarily steering them towards illegal activities. Our research [30], [55] into various game-cheating communities indicates that these platforms serve as fertile ground for cheating enthusiasts to enhance their skills. For instance, James from the *CS:GO* cheating community found these communities enriching, stating, "I've learned to program entirely from cheating communities. It's kind of amazing in a way. The right parts of these toxic communities can teach me things that I wasn't able to learn on my own. Sure we make cheats, but we also write various libraries that can be used in standard java projects some of which are actually very impressive". He further highlighted the potential professional opportunities that emerged from his expertise in this area, helping him receive "several possible job offers for cheats and other things".

As individuals immerse themselves in these communities and expand their skill sets, they often encounter diverse social experiences which not only elevate their gaming capabilities [6], [58] but also allow for networking. Some might come across private forums or even engage in grey-area activities. Michael recounts his experience operating a game server dedicated to cheats, which was initially financed through a platform known for DDoS-for-hire services funded by credit card fraud. He asserts that he is no longer involved in these activities. With regard to cybercrime, similar patterns of influence and learning can be seen, both online [67] and offline [21]. For example, some get introduced to aspects of cybercrime through offline social influences, such as collaborating on installing surveillance software in university labs [68]. Online settings present numerous opportunities for enthusiasts to learn about hacking and related domains. However, it is important to

underscore that participation in a cheating community does not ensure cybercriminal engagement, and many remain enthusiasts without crossing these legal boundaries. Tim claims that developing cheats is enjoyable for those interested in reverse engineering and security engineering, stating, "It's really just fun to work on".

5) The Veil of Anonymity: Derived from the motivation component of RAT, it is clear that anonymity in digital environments plays a pivotal role in user behaviours, particularly regarding actions that may have negative consequences. Game scholars [69] have noted that the construction of identity in digital spaces often diverges from its real-world equivalent. Chen and Wu [51] found that anonymous identities that users adopt in game platforms create a sense of diminished repercussions for cheating, while the likelihood to cheat increases with players' interactions with anonymous individuals.

The importance of anonymity is widely evident within cybercrime. For instance, one strategy involves using Tor networks or VPNs to mask IP addresses and location, providing a level of obfuscation while conducting illicit activities online. Cybercriminals also do business in cryptocurrencies, reducing the traceability of transactions by law enforcement. Users typically adopt pseudonymous nicknames, which allow them to carve out a reputation or brand within the community [70], while shielding them from direct associations with their real-world identities and potential legal implications. This dual nature is a delicately balanced strategy: it requires building a reputation while also remaining hidden.

B. Unique Characteristics in Cheating

Through our application of RAT, it became apparent that cheating in gaming brings forth some elements not commonly observed in broader cybercriminal activities. First, it is important to highlight the intrinsic motivation and dedication that gamers, including cheaters, hold for the art and development of gaming. As a former cheat developer articulates, "You can try to remove them from the [gaming] ecosystem but they are [still] players" [71]. Cheaters may even feel a deeper passion and connection to games than the game publishers exhibit. Some of the motivation for cheating are tied to when game updates are limited or vulnerabilities remain unaddressed [56]. In contrast, profit-driven cybercriminals may lack this deep-rooted connection to their targets. Their primary motivations are external, often rooted in monetary gains.

Tied to this, cheating introduces an element of entertainment and innovation that stimulates players' curiosity. Many cheaters begin their journey as standard players, only to grow disillusioned or bored over time. This can lead them to engage in "meta-gaming", which shifts their objectives: instead of playing by the game's original rules, they challenge themselves to overcome the underlying systems of a game. It is akin to identifying zero-day vulnerabilities [72] or modifying a game to enhance its original features [73]. Max encapsulates this sentiment noting, "everyone can win when cheating, it's not a challenge. The challenge in cheating for me at least is writing the software and finding ways to go around the anticheat to not get banned". Although recreational hacking for its own sake does exist in cybercriminal contexts, it is relatively a niche endeavour, particularly in the face of increasing legal consequences [21].

VII. Discussion

Using the emergent themes from interviews and existing literature, we applied RAT to the context of game cheating to analyse themes that parallel those in cybercrime. In this section, we delve into the implications of the findings for the cyber security sector, and how our findings can inform law enforcement regarding potential interventions.

A. The Cyber Security Mindset

Our examination of RAT and the parallels between cheating and cybercrime illuminates the attack and defence dynamic, which is central to cyber security. This suggests its relevance lies not only in the technical details but also in the underlying motivations, perceptions, and social dynamics driving these actions. The thought processes and motivations behind cheating offer a glimpse into an environment where such actions are both understood and sometimes even promoted. However, it is crucial to note that this does not mean every individual involved in cheating would naturally gravitate towards malicious cyber activities. Often, the broader discourse has overlooked these nuances, leading to an oversimplified view of game cheating as merely malicious, without considering the broader context in which it occurs. There are examples where one's skills and experiences have been leveraged for alternative means, such as some cheat developers who transitioned their roles to anti-cheat development, aiding gaming companies and enjoying greater rewards for themselves [71]. These cases reflect an average users' well-intentioned ability to be a "part of the solution" rather than "the problem" [74].

Cheating skillsets and mindsets could be transferable to cyber security. For instance, some young individuals who are adept at identifying unconventional approaches to problem-solving may positively contribute their skills to the cyber security industry. Many players often aim to gain skills, knowledge, and experience to progress in games, which together with pre-existing knowledge in security, can be synergised for more advanced training in cyber security [6]. Based on these aspects, security companies could consider game cheaters as potential talented recruits for cyber security. Gamification is already a popular approach in the field of HCI to aid user learning and engagement, and there already exist games that seek to teach real-world problem-solving skills related to cyber security (e.g., *ThreatGEN®: Red vs. Blue*[3] [75]). Through the gamification of real-world resource elements that align with online gaming, companies can leverage the transferable skills acquired through game cheating to support socially beneficial initiatives. With the ongoing skills gap in cyber security, there is a need for proactive policies that identify and nurture

[3]An online multi-player strategy game introduced in 2019, where a single player competes against the computer AI or live players in head-to-head matches attacking and defending computer networks.

such talent. Much in the same way startup incubators provide young or early-stage entrepreneurs with a space to develop their ideas, providing this alternative space can potentially renavigate the motivations of these individuals towards more pro-social means in the cyber security industry.

B. Implications on the Cybercriminal Engagement

In exploring cheating, we observed various social and technical characteristics that align with with cybercrime, such as the tendency to prioritise objectives and bypass established rules and norms. Our analysis indicated that some cheaters, while not always directly involved in cybercriminal activities, do come into contact with those who are. This suggests that, even without active participation, there is a potential for cheaters to become accustomed to elements of cybercrime under the guise of merely progressing in their cheating efforts. As we revisit the claim regarding the potential link between the two domains [1], [2], it is clear that both the direct and perceived interactions with cybercrime have implications for the potential trajectories of users.

While our study does not directly evaluate the 'pathway' claim, it provides an initial exploration through the examination of shared themes, and expands our understanding of the implications arising from any association. The findings highlight the need for future research to simultaneously investigate these broader implications, diverging from the adversarial stance often adopted by game companies towards cheating. This holistic approach could offer a more comprehensive understanding of the intricate interplay between cheating and cybercrime. In addition, our findings deviate from the linear trajectory outlined in the NCA's report [2], instead suggesting a more sporadic and context-dependent development. It is particularly concerning how, in their playful quest to cheat in a game, players might unknowingly tread the boundaries of cybercrime. Even when they do become aware, the allure of financial gains or the security provided by these underground communities might be strong. Therefore, some players, particularly those unfamiliar with security concepts or the legal implications of cybercrime, may inadvertently find themselves on the fringes of these activities without fully grasping the gravity of their involvement. Given the vast number of young individuals engaged in gaming [76], the potential for such unintended exposures warrants further attention beyond the gaming industry.

The findings provide fundamental insights regarding the shared characteristics that could be incorporated in informing future interventions. However, it is important to note that while the study offers insights into these associations, establishing a definitive causal link requires more in-depth longitudinal research. Additionally, the findings underscore the need to proactively identify potentially vulnerable users who may inadvertently encounter cybercrime-related activities. Future investigations can delve into the temporal aspects and trajectories over time, allowing for a more comprehensive understanding of how engagement in gaming and cheating might or might not lead to subsequent involvement in cybercrime.

C. Methodological Limitations

The study draws data from a limited set of games, indicating that they might not fully represent the broader gaming community. While certain unique attributes of specific games may not have been encompassed in this study, our methodology enabled us to garner insights into some of the industry's most popular games over the past decade. Our systematic literature review also allowed us to extend our findings beyond those games captured in the interview dataset. A related limitation of this study is that we focused on a particular type of cheating involving automated scripts to break the rules. However, other forms of transgressive play [46] which are sometimes also recognised as a form of cheating were not explored. Investigating the nuances of game cheating necessitates addressing these challenges, and how much they are covered by RAT or extend beyond it. Future data collection could incorporate a broader spectrum of games, and transgressive play, potentially spanning distinct game genres, or examining various competitive game genres to discern how cheating dynamics differ across these diverse contexts and behaviours [77].

In examining our sample, we found that participants' engagement with cheating extends beyond mere gameplay, reflecting diverse interactions withgames. This variation is further complicated by the fact that some participants have well-defined roles, while others are involved in related activities without formal recognition. This may stem from their perception of their involvement as non-professional or low commitment, with gameplay being their primary connection to the game. The variety of modes of engagement, and their varying levels of commitment present a challenge in distinctly categorising them. As a result, for the scope of this study, we concentrated on their shared interest and experience in gameplay. However, future research could benefit from a more focused investigation into specific formal or informal roles, such as moderators, to explore whether their experiences significantly differ from those of general players.

D. Limitations of Applying RAT to Game Cheating

Owing to its foundation in offline criminology, scholars have previously questioned how neatly RAT can be applied to the online medium [19]. Given the limited scope of this study, RAT stands as an appropriate initial framework for gaining insights into the cheater's perspective, and exploring parallels with cybercrime. Future research could explore whether there is a need to modify RAT, or develop a new theoretical framework, fitted to context-specific online environments. The interview dataset that was subject to our secondary analysis also limited our ability to engage fully with some aspects of RAT. In our analysis of the 'lack of guardians' component, we noted that the data does not extend to the scope of law enforcement interventions in cybercrime. This limitation arises from our interview questions and methodology being chiefly focused on aspects directly tied to gaming. Therefore, this research focus is indicative of the specific scope of our studies,

rather than a reflection of the participants' lack of awareness of the active measures law enforcement is taking to address related underground activities.

VIII. Conclusion

This study explored the parallels between game cheating and cybercrime by applying Routine Activity Theory. Our findings shed light on previously overlooked themes in the game cheating/cybercrime narrative, including the victory-oriented perspective, exploitation of user and system integrity, attack-defence dynamic, social immersion and domain familiarisation, and anonymity.

There are two key implications which surface from the analysis. First, some cheaters may unknowingly interact with malicious elements, such as intermittent engagement with malware or familiarisation with cybercriminals, as a part of their endeavour to cheat. These individuals may not fully grasp the severity of their actions, or the potential for greater real-world risks. There is a need to closely monitor the environments in which users may inadvertently be exposed to cybercrime. Secondly, our findings indicate that the urge to cheat often stems from players' curiosity and their drive to innovate, aiming to overcome the repetitive challenges presented by game designers. Discovering vulnerabilities and avenues of exploitation then becomes a meta-game in itself, delivering an engaging experience for the cheaters.

Based on the findings, we highlight the possibility of steering game cheaters towards more pro-social practices in the cyber security industry, while monitoring the unintended exposure of users to the context of cybercrime. Overall, the study underscores the need for continued investigation to understand the nuances, and make informed decisions surrounding the possible link between game cheating and cybercrime. These insights encourage moving beyond the limited view of a simple progression between game cheating and cybercrime to a more comprehensive, and context-specific, understanding.

References

[1] National Cyber Crime Unit / Prevent Team, *Pathways into cybercrime.*, ser. Intelligence Assessment. National Crime Agency, 1 2017, https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file.

[2] CREST and National Crime Agency, *Identify, Intervene, Inspire – Helping Young People to Pursue Careers in Cyber Security, Not Cyber Crime.* CREST, 2015, https://www.nationalcrimeagency.gov.uk/who-we-are/publications/623-cyber-crime-report-crest-nca/file.

[3] E. J. Hayes, "Playing it safe: Avoiding online gaming risks," *US-CERT*, 2006, https://www.cisa.gov/uscert/sites/default/files/publications/gaming.pdf.

[4] S. Pontiroli, *The cake is a lie! Uncovering the secret world of malware-like cheats in video games*, Virus Bulletin Conference, 2019, https://www.virusbulletin.com/virusbulletin/2020/02/vb2019-paper-cake-lie-uncovering-secret-world-malware-cheats-video-games/.

[5] J. Yan and B. Randell, "A systematic classification of cheating in online games," in *Proceedings of 4th ACM SIGCOMM Workshop on Network and System Support for Games*, ser. NetGames '05. New York, NY, USA: ACM, 2005, p. 1–9.

[6] M. Consalvo, *Cheating: Gaining Advantage in Videogames*. The MIT Press, 2007.

[7] P. Karkallis, J. Blasco, G. Suarez-Tangil, and S. Pastrana, "Detecting video-game injectors exchanged in game cheating communities," in *Computer Security – ESORICS 2021*, E. Bertino, H. Shulman, and M. Waidner, Eds. Cham: Springer International Publishing, 2021, p. 305–324.

[8] Activision and Blizzard, *Cheating Cheaters: Malware Delivered as Call of Duty Cheats*, 3 2021, https://research.activision.com/publications/2021/03/cheating-cheaters-malware-delivered-as-call-of-duty-cheats.

[9] L. E. Cohen and M. Felson, "Social change and crime rate trends: A routine activity approach (1979)," in *Classics in environmental criminology*. Routledge, 2010, pp. 203–232.

[10] Irdeto, *Irdeto Global Gaming Survey: The last checkpoint for cheating*, 2018, https://resources.irdeto.com/irdeto-global-gaming-survey/irdeto-global-gaming-survey-report-2.

[11] M. Humphries, "South korea makes game hacking illegal," Dec 2016, https://www.pcmag.com/news/south-korea-makes-game-hacking-illegal.

[12] Kaspersky, "Analytical report on gaming-related cyberthreats in 2020-2021," Aug 2021, https://securelist.com/game-related-cyberthreats/103675/.

[13] H. Unterbrink, "Cheating the cheater: How adversaries are using backdoored video game cheat engines and modding tools," 2021, http://blog.talosintelligence.com/2021/03/cheating-cheater-how-adversaries-are.html.

[14] M. Yar, "The novelty of 'cybercrime': An assessment in light of routine activity theory," *European Journal of Criminology*, vol. 2, no. 4, pp. 407–427, 2005.

[15] A. K. Ghazi-Tehrani and H. N. Pontell, "Phishing evolves: Analyzing the enduring cybercrime," *Victims & Offenders*, vol. 16, no. 3, p. 316–342, Apr 2021.

[16] T. J. Holt and A. M. Bossler, "Examining the applicability of lifestyle-routine activities theory for cybercrime victimization," *Deviant behavior*, vol. 30, no. 1, pp. 1–25, 2008.

[17] F. T. Ngo and R. Paternoster, "Cybercrime victimization: An examination of individual and situational level factors," *International Journal of Cyber Criminology*, vol. 5, no. 1, p. 773, 2011.

[18] J. Van Wilsem, "'Bought it, but never got it': Assessing risk factors for online consumer fraud victimization," *European sociological review*, vol. 29, no. 2, pp. 168–178, 2013.

[19] E. R. Leukfeldt and M. Yar, "Applying routine activity theory to cybercrime: A theoretical and empirical analysis," *Deviant Behavior*, vol. 37, no. 3, p. 263–280, Mar 2016.

[20] M. M and D. Samantha, "Cyber crime: A review of the evidence - chapter 1: Cyber-dependent crimes," *Home Office Research Report 75*, p. 35, 2013, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf.

[21] J. Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime*. Harvard University Press, Oct 2018.

[22] A. Goldsmith and D. S. Wall, "The seductions of cybercrime: Adolescence and the thrills of digital transgression," *European Journal of Criminology*, vol. 19, no. 1, p. 98–117, Jan 2022.

[23] A. M. Bossler and T. J. Holt, "On-line activities, guardianship, and malware infection: An examination of routine activities theory." *International Journal of Cyber Criminology*, vol. 3, no. 1, 2009.

[24] T. J. Holt, J. R. Lee, J. D. Freilich, S. M. Chermak, J. M. Bauer, R. Shillair, and A. Ross, "An exploratory analysis of the characteristics of ideologically motivated cyberattacks," *Terrorism and political violence*, vol. 34, no. 7, pp. 1305–1320, 2022.

[25] J. Heaton, *Reworking qualitative data*. Sage, 2004.

[26] ——, "Secondary analysis of qualitative data," *Social Research Methods*, p. 506, 1998.

[27] C. Hakim, "Secondary analysis and the relationship between official and academic social research," *Sociology*, vol. 16, no. 1, pp. 12–28, 1982.

[28] Anonymous, "Unpublished," *Manuscript submitted for publication*, 2023.

[29] S. Cho and I. Flechais, "Cheating the cheaters: A look inside the toxic culture of game cheating communities," in *Proceedings of the 2022 Digital Games Research Association (DiGRA) International Conference*, 2022.

[30] S. Cho, J. Lusthaus, and I. Flechais, "Unpacking the dynamics of harm in game cheating communities: A guiding framework for cross-industry intervention," *ACM Games: Research and Practice*, 2024, Forthcoming.

[31] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within

the software engineering domain," *Journal of systems and software*, vol. 80, no. 4, pp. 571–583, 2007.
[32] M. Dixon-Woods, S. Agarwal, D. Jones, B. Young, and A. Sutton, "Synthesising qualitative and quantitative evidence: a review of possible methods," *Journal of health services research & policy*, vol. 10, no. 1, pp. 45–53, 2005.
[33] G. W. Noblit, R. D. Hare, and R. D. Hare, *Meta-ethnography: Synthesizing qualitative studies*. sage, 1988, vol. 11.
[34] G. Paré, M.-C. Trudel, M. Jaana, and S. Kitsiou, "Synthesizing information systems knowledge: A typology of literature reviews," *Information & Management*, vol. 52, no. 2, pp. 183–199, 2015.
[35] J. Blackburn, R. Simha, N. Kourtellis, X. Zuo, M. Ripeanu, J. Skvoretz, and A. Iamnitchi, "Branded with a Scarlet "C": Cheaters in a Gaming Social Network," in *Proceedings of the 21st International Conference on World Wide Web*, ser. WWW '12. New York, NY, USA: Association for Computing Machinery, 2012, p. 81–90.
[36] V. H. H. Chen and J. Ong, "The rationalization process of online game cheating behaviors," *Information, Communication & Society*, vol. 21, no. 2, p. 273–287, Feb 2018.
[37] L. H. Doyle, "Synthesis through meta-ethnography: paradoxes, enhancements, and possibilities," *Qualitative Research*, vol. 3, no. 3, pp. 321–344, 2003.
[38] A. K. Cobb and J. N. Hagemaster, "Ten criteria for evaluating qualitative research proposals," pp. 138–143, 1987.
[39] V. Braun and V. Clarke, *Thematic analysis.* American Psychological Association, 2012.
[40] ——, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.
[41] M. E. Kiger and L. Varpio, "Thematic analysis of qualitative data: Amee guide no. 131," *Medical teacher*, vol. 42, no. 8, pp. 846–854, 2020.
[42] L. Varpio, R. Ajjawi, L. V. Monrouxe, B. C. O'Brien, and C. E. Rees, "Shedding the cobra effect: problematising thematic emergence, triangulation, saturation and member checking," *Medical education*, vol. 51, no. 1, pp. 40–50, 2017.
[43] J. Thomas and A. Harden, "Methods for the thematic synthesis of qualitative research in systematic reviews," *BMC Medical Research Methodology*, vol. 8, no. 1, pp. 1–10, 2008.
[44] L. A. Sparrow, M. Gibbs, and M. Arnold, "The ethics of multiplayer game design and community management: Industry perspectives and challenges," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Yokohama Japan: ACM, May 2021, p. 1–13.
[45] T. E. Mortensen, J. Linderoth, and A. M. Brown, *The dark side of game play: Controversial issues in playful environments*. Routledge, 2015.
[46] A. F. Meades, *Understanding Counterplay in Video Games*. Routledge, Jun 2015.
[47] L. Wang, L. Fan, and S. Bae, "How to persuade an online gamer to give up cheating? uniting elaboration likelihood model and signaling theory," *Computers in Human Behavior*, vol. 96, p. 149–162, Jul 2019.
[48] D. A. Fields and Y. B. Kafai, "'Stealing From Grandma' or generating cultural knowledge? contestations and effects of cheating in a tween virtual world," *Games and Culture*, vol. 5, no. 1, pp. 64–87, 2010.
[49] S. V. Irwin and A. Naweed, "Bm'ing, throwing, bug exploiting, and other forms of (un)sportsmanlike behavior in CS:GO esports," *Games and Culture*, vol. 15, no. 4, p. 411–433, Jun 2020.
[50] D. D. Dumitrica, "An exploration of cheating in a virtual gaming world," *Journal of Gaming & Virtual Worlds*, vol. 3, no. 1, pp. 21–36, 2011.
[51] V. H. H. Chen and Y. Wu, "Group identification as a mediator of the effect of players' anonymity on cheating in online games," *Behaviour & Information Technology*, vol. 34, no. 7, pp. 658–667, 2015.
[52] A. Boldi and A. Rapp, "'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*, pp. 1–21, 2023.
[53] S. De Paoli and A. Kerr, "'We will always be one step ahead of them' A case study on the economy of cheating in MMORPGs," *Journal of Virtual Worlds Research*, vol. 2, no. 4, 2010.
[54] Y. Wu, J. Hu, and W. Li, "The link between online gaming behaviour and unethical decision-making in emerging adults: the mediating roles of game cheating and moral disengagement," *Behaviour & Information Technology*, vol. 0, no. 0, p. 1–14, Jun 2022.
[55] S. Cho, "A community-based investigation of competitive cheating," in *Extended Abstracts of the 2022 Annual Symposium on Computer-Human Interaction in Play*, ser. CHI PLAY '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 367–369.
[56] ——, "A community-based investigation of cheating in online multiplayer games," Ph.D. dissertation, University of Oxford, 2023.
[57] G. Frasca, "Simulation versus narrative: Introduction to ludology," in *The video game theory reader*. Routledge, 2013, pp. 221–235.
[58] C. A. Lindley, "Game taxonomies: A high level framework for game analysis and design," *Gamasutra feature article*, vol. 3, 2003, https://www.gamedeveloper.com/design/game-taxonomies-a-high-level-framework-for-game-analysis-and-design.
[59] J. Lusthaus, J. Van Oss, and P. Amann, "The Gozi group: A criminal firm in cyberspace?" *European Journal of Criminology*, vol. 20, no. 5, pp. 1701–1718, 2023.
[60] T. J. Holt, R. Leukfeldt, and S. van de Weijer, "An examination of motivation and routine activity theory to account for cyberattacks against dutch web sites," *Criminal Justice and Behavior*, vol. 47, no. 4, pp. 487–505, 2020.
[61] M. Sauter, "'LOIC will tear us apart': The impact of tool design and media portrayals in the success of activist DDOS attacks," *American Behavioral Scientist*, vol. 57, no. 7, pp. 983–1007, 2013.
[62] D. Callele, E. Neufeld, and K. Schneider, "Requirements in conflict: Player vs. designer vs. cheater," in *2008 Third International Workshop on Multimedia and Enjoyable Requirements Engineering - Beyond Mere Descriptions and with More Fun and Games*, Sep 2008, p. 12–21.
[63] J. Lusthaus, E. Kleemans, R. Leukfeldt, M. Levi, and T. Holt, "Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions," *Trends in Organized Crime*, pp. 1–24, 2023.
[64] B. Biswas, A. Mukhopadhyay, and G. Gupta, "'Leadership in action: How top hackers behave': A big-data approach with text-mining and sentiment analysis," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, vol. 9, 2018.
[65] J. Hughes, B. Collier, and A. Hutchings, "From playing games to committing crimes: A multi-technique approach to predicting key actors on an online gaming forum," in *2019 APWG Symposium on Electronic Crime Research (eCrime)*, 2019, pp. 1–12.
[66] S. Pastrana, A. Hutchings, A. Caines, and P. Buttery, "Characterizing eve: Analysing cybercrime actors in a large underground forum," in *Research in Attacks, Intrusions, and Defenses*, M. Bailey, T. Holz, M. Stamatogiannakis, and S. Ioannidis, Eds. Cham: Springer International Publishing, 2018, pp. 207–227.
[67] V. Benjamin, W. Li, T. Holt, and H. Chen, "Exploring threats and vulnerabilities in hacker web: Forums, irc and carding shops," in *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)*, May 2015, p. 85–90.
[68] A. Hutchings, "Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission," *Crime, Law and Social Change*, vol. 62, no. 1, p. 1–20, Aug 2014.
[69] M. Sicart, *The Ethics of Computer Games*. Cambridge, Mass.: The MIT Press, Aug 2011.
[70] E. R. Leukfeldt and T. J. Holt, "Cybercrime on the menu? examining cafeteria-style offending among financially motivated cybercriminals," *Computers in Human Behavior*, vol. 126, p. 106979, 2022.
[71] M. Minotti, "Game makers need to keep up with cheaters," 11 2021, https://venturebeat.com/2021/11/09/game-makers-need-to-keep-up-with-cheaters/.
[72] L. Auriemma and D. Ferrante, *Game Engines: A 0-Day's Tale*, May 2013, http://revuln.com/files/ReVuln_Game_Engines_0days_tale.pdf.
[73] J. Donnelly, "The half-life mod that took 17 years to land on steam," May 2016, https://www.eurogamer.net/articles/2016-05-01-the-half-life-mod-that-took-17-years-to-land-on-steam.
[74] V. Zimmermann and K. Renaud, "Moving from a "human-as-problem"' to a "human-as-solution" cybersecurity mindset," *International Journal of Human-Computer Studies*, vol. 131, pp. 169–187, 2019.
[75] ThreatGEN, "ThreatGEN® Red vs. Blue cybersecurity gamification," https://threatgen.com/solutions/.
[76] A. K. Przybylski and N. Weinstein, "A large-scale test of the goldilocks hypothesis: Quantifying the relations between digital-screen use and the mental well-being of adolescents," *Psychological Science*, vol. 28, no. 2, p. 204–215, 2 2017.
[77] J. Paay, J. Kjeldskov, D. Internicola, and M. Thomasen, "Motivations and practices for cheating in Pokémon GO," in *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile*

Devices and Services - MobileHCI '18. Barcelona, Spain: ACM Press, 2018, p. 1–13.

APPENDIX

Interview Protocol for Study A

The following questions pertained to users of the game cheating communities. For participants who had specialised experiences, such as a cheat developer or an entrepreneur, we suited the questions along with the contents of the responses they provided during the interviews.

- To start off, could you tell me about your experience with cheat communities? Which websites (and for which games, if anything besides CS:GO) have you had experience with? Could you specify whether you were part of public or invitation-only ones?
- When and how did you join this cheating community? What motivated you in the first place, and how did you go about finding those websites that you frequent?
- Having been involved for these years, how would you justify someone to be a true 'member' of a cheat community? (e.g., Is it about how frequently you contribute? Whether you have developed something before?)
- Have you formed friendships or business partnerships with others through any of these platforms? Could you provide an example of how you developed an online bond with someone within the community?
- How do you establish trust with others in this community? Conversely, in what ways do you find it difficult to trust others?
- Have you ever assumed any specific roles within the community? If so, how did you attain these roles, and what responsibilities did they entail on a day-to-day basis? (e.g., whether it's for purposes of discussion, marketplace, or something else)
  - Staff: Did you need to go through an application process?
  - Cheat developer/administrator: What administrative process is involved in the set-up phase?
  - Have you ever recruited anyone else?
  - Were you financially compensated for your work?
- Have you familiarised yourself with the rules outlined in the channels? What guiding principles were employed in establishing these rules?
- Have you personally experienced being banned from the community, or have you witnessed any of your friends facing such consequences?
- Have you ever been involved in trolling or griefing others? Could you provide an example?
- Based on your experience and/or observations of others, what is the common convention around the usernames? Do most players use same usernames across different platforms?
- What attracts you to this cheating community, besides its relevance to cheating?

Interview Protocol for Study B

The choice of the word between *modding* and *cheating* varied depending on the experience of the game in question and the experience of the player. The authors of this work are aware that there are a lot of sensitivity around associating these terms with cheating. During our case selection for the games, we included uses of the terms 'modding' and 'mods' that refer specifically to *unauthorised* alterations to a game, which aligns with the scope of cheating in this study.

- How long have you been involved in cheating/modding in [the game]?
- Do you recall what made you want to cheat/mod in this game the very first time?
- Can you briefly explain what cheating/modding in [the game] entails from your experience? Are there any specific features you prefer or frequent from the cheats/ mods you have used?
- What do you look for in a cheat/mod? If there are several similar ones in the market, how do you make your choice?
- Do you find it fun to cheat/mod? If so, exactly what part of it do you enjoy the most?
- Is there anything you would like to see changed or introduced by the game developers in relation to your experience cheating/modding?

Optional Post-interview Survey

I would like to contextualise our conversation by answering the following. However, these are completely optional, and you can refuse to answer only some, all, or none.

- Gender:
- Age:
- Student or working professional:
- Base country: