

Predicting Game Cheating Behavior Through the Social Network

Early stage paper

Richard Alvarez
University of Texas at San Antonio
richard.alvarez@utsa.edu

Paras Bhatt
University of Texas at San Antonio
paras.bhatt@utsa.edu

Dorde Klisura
University of Texas at San Antonio
dorde.klisura@utsa.edu

Kim-Kwang Raymond Choo
University of Texas at San Antonio
raymond.choo@fulbrightmail.org

ABSTRACT

Cheating behavior is a major security threat for online gaming, ranging from a minor unfair advantage in game to completely disabling victim systems and identity theft. In this paper, we propose a social network analysis study on Steam users banned for cheating on the online platform. We will collect the identified cheater's data from a social network with a depth of $n+3$ and identify user descriptive characteristics that are correlated with the contagion effect of cheating behavior. These characteristics will then serve as inputs to develop a cheating probability ratio that will be tested on future user social networks.

Keywords

Social network contagion, online cheating behavior, steam

INTRODUCTION

Cheating represents a cybersecurity threat that can range from unfair gameplay advantages to identity theft and compromised systems. In a 2022 study, Kaspersky Labs, a cybersecurity firm, found *thousands* of fake cheat code programs that disable systems and steal user data. (Holpuch, 2022). As an online industry, gaming is expected to be valued at \$365.6 Billion dollars in 2023, up from \$180.1 Billion dollars in 2021 (Statista, 2023, Madhurja & Siddique, 2020); thus

representing an enticing target for malicious users and an important domain to research the cheating problem.

Cheaters do not interact in a vacuum. Users generally interact with anonymous players as they cooperate or compete, sometimes even becoming anonymous friends on the social network. Current research on cheating behavior has shown anonymity and social networks play an integral role in determining characteristics of cheating (Christensen et al., 2013; Jeff & Choi, 2002; Saarinen, 2017; Yan & Randell, 2005), the psychology behind cheating (Ladanyi & Doyle-Portillo, 2017; Wu & Chen, 2018), and the relationship between cheaters and users (Blackburn et al., 2014; Woo et al., 2018; Wu & Chen, 2013; Zuo et al., 2016) related to individuals within a social network. Of note, research done by Blackburn et al. (2014) found that non-cheaters had no friends who were known cheaters, and 15% of cheaters had other cheaters as friends. Essentially, what this means is when a cheater is identified in a social network, players who do not cheat will self-select themselves out of the cheaters social network. Given the understanding that cheaters were more likely to have other cheating friends in their network we reason that the social network of a known cheater can be leveraged to predict whether individuals in the network cheat due to the network theory, the contagion effect.

By applying contagion theory to the player's social network this paper proposes the following research questions:

How can a cheater's social network be leveraged to identify unknown cheating individuals within the network? How can a cheating network be leveraged to find cheaters?

To tackle this research question, we revisit the data collection process conducted by Blackburn et al. (2014) and conduct a temporal study of cheating user's social network who were caught and

banned on the Steam gaming platform. Using a recently banned individual as a baseline, we then expanded data collection to all users in their social network with a distance of $n+3$ from the initial user. That is a three-friend distance or a friend of a friend of a friend of the initial user. We then extend the study by taking a structural equation modeling approach to model an individual's social characteristics onto existing social persuasive constructs identified in the information systems (IS) literature; these factors will become the predictors of cheating behavior. Finally, we develop a cheating likelihood equation for managers to predict the likelihood a flagged account is cheating. Our study differentiates itself from past research in that our focus is on identifying qualitative predictive factors among individuals in social networks, rather than simply providing a surface-level view of the social network. Thus, this paper proceeds as follows. First, the paper defines cheating, and the behaviors related to cheating. Next, the paper covers current research on the social aspect of cheating. Third, the paper briefly discusses network theory with a focus on the contagion effect model. Finally, we discuss the methodology chosen followed by the results and discussion of our study.

LITERATURE REVIEW

Cheating social behaviors

In this study, we follow Woo et al. (2018) to define and study cheating behaviors that are enabled through and identified using social network structures. Considerable research has looked at the social relationships between players and known cheaters (Blackburn et al., 2014; Blackburn et al., 2012; Zuo et al., 2016). On one study, a group of known cheating game accounts were reviewed on the Steam service. Steam allows players to interact with each other and play together in a variety of different games. The study sought to understand the propagation of cheaters in a social network over time. One study found that “nearly 70% of non-cheaters have no friends who are cheaters” (Blackburn et al., 2014, pg. 5). Unsurprisingly if a cheater is identified within their social network,

non-cheating friends of cheaters would expunge the cheater from their social network. The study concluded with a second surprising finding, the likelihood of engaging in cheating behavior was impacted by the number of cheating friends an individual has. The more cheating friends a fair player has, the more likely they are to engage in cheating behavior. One suggested reason for this finding is attributed to the delay between when the cheat was performed and when the individual was caught. The gap between the two events leads members of the social network to observe the reward from engaging in cheating behaviors but not the losses incurred from being caught. Furthermore, the results found cheating players who were marked for cheating but not banned were more likely to hide their account from public view when caught strongly suggesting that cheaters are wary of the social stigma of being outed to their peers.

A similar study applied social cognitive theory to online cheating behavior to support the findings above (Wu & Chen, 2013). For a quick refresher, social cognitive theory proposes that an individual's learned behavior is not exclusively a result of personal factors but a combination of personal, environmental, and behavioral factors (Bandura, 1999; Schunk & Zimmerman, 1997). In the context of an online game environment, this suggests that cheating is not simply an ingrained desire but influenced by social pressures. Findings from a survey sample of 1746 online gamers from China and India suggested that social cognitive theory explained that social external and internal factors impacted the likelihood of an individual engaging in cheating behavior. In particular, the individual's social environment, their own personal views on cheating behavior, and the potential reward for engaging in illicit cheating online. Of interest, the more a peer saw cheating behavior go unpunished the more likely the individual was to engage in cheating behavior, confirming the findings above. Surprisingly, an individual does not measure their own ability in the mental calculus of cheating behavior, rather the perceived individual skill had no significant

measure on whether a person decides to engage in cheating. The findings suggest that the level of security and anti-cheating programs do not deter attempts to engage in the behavior.

Summarily, multiplayer online game research has made significant strides in explaining the potential motivation for cheating, the deterrents for doing so, and the social relationships between players and cheaters in these environments. Specifically, research shows that among other factors, players have a significant impact on each other when influencing cheating behavior.

Social constructs and their application in Information Systems

In psychology literature, Robert Cialdini identified seven (7) principles of persuasion that influence an individual's behavior patterns. Cialdini's 2008 research has been applied quite extensively in IS literature. For example, the impact of authority on online shopping purchases (Yi-Hsiu Cheng and Hui-Yi Hob 2014), and another study on the scarcity impact on observed panic buying behavior on e-purchases (Kum Fai Yuen et al., 2022). Yet another study looked at reciprocation on the degree of self-disclosures for professionals in an online community (Posley et al. 2010).

For our study, we are primarily focused on identifying the constructs of *unity and social proofing* principles within the social network. The principle of unity refers to the synchronous performance of individuals engaging in an experience or activity together (EX. Gaming, Dancing, Classmates. From these experiences, individuals will exhibit increased influence over each other to adopt similar behaviors or agree with one another (Cialdini 2008). In one such work, researchers followed players' "unity" behaviors in games such as World of Warcraft (WoW) and Counter-Strike (CS) (Frostling-Henningsson 2019). The results of the study revealed online gaming is motivated by social reasons, creating situations for cooperation and communication. In additional studies, cybersecurity researchers found not only that "unity" type messaging in cybersecurity

training was more effective at encouraging compliance than authority-type messaging; but also quantified susceptibility to unity, social proof type messaging (Vargheese et al. 2020, Vargheese et al. 2022).

Social proofing, on the other hand, refers to the tendency of an individual to agree and behave in a manner that is considered acceptable within the individual’s social group (Cialdini 2008). The social proof principle of influence is well-researched in IS (Roethke et al. 2020, Klumpe et al 2018). In one such study, researchers leveraged machine learning to identify individuals who are susceptible to social proofing linguistics technics (Braca & Dondio 2023). Another study observed the ability of social media to generate social proof causing stockpiling behavior during the covid-19 pandemic (Muhammad Naeem 2021).

Cialdini’s Persuasion Principles	Definition	Examples in IS
Likability	An individual will prefer the opinion of someone they like or are familiar with.	Cori Faklaris 2018 Lins & Sunyaev 2022
Reciprocity	Individuals attempt to pay back or “reciprocate” in kind, what another individual has given them.	Helio et al. 2011 Posley et al. 2010
Authority	Individuals are inclined to automatically obey perceived authority	Amblee & Bui 2011 Cheng & Hobb 2014
Social Proof	Individuals will follow what other individuals are doing	Roethke et al. 2020 Klumpe et al. 2018 Braca & Dondio 2023
Consistency/Commitment	Individuals are driven to remain consistent with past behaviors	Liao et al. 2020 Shih et al. 2023 Teng et al. 2016
Scarcity	Individuals will desire something more if access to it is limited.	Yuen et al. 2022
Unity	Individuals who engage in tasks together are driven to developed shared identity	Frostling-Henningsson 2019

Table 1. Cialdini’s Persuasion Principles and their applications in information systems

Social networks and the contagion effect

Social networks are well studied in human sociology (Contractor & DeChurch, 2014; Hill & Dunbar, 2003; Krause et al., 2007; Scott, 1988). Within the larger web of human interactions, social networks refer to the connections and nodes that reflect the interconnected relationships between individuals.

In these networks, several individuals will adopt traits and characteristics of the larger group in a network. How these characteristics move through the network is called the contagion effect. The contagion effect refers to an individual mimicking the behavior of another as the behavior spreads through a network. Significant research has already gone into mapping the spreading of these contagions through a network (Eskine et al., 2013; Nacos, 2020; Zhao et al., 2010). For example, in a medical study, it was found that negative behaviors such as drinking and smoking can spread through a social network (Christakis & Fowler, 2013).

In another study on Twitter users, research has shown that the spread of behaviors is not geographically limited and can spread just as easily online as in person; however the propagation of behaviors is impacted by the degree of social distance or path length between individuals in a social network. (Fabrega & Paredes, 2013). The path length refers to the degree of separation between two individuals in a social network.

To give an example of this model, imagine browsing through the Facebook profile of the individual Adam. Adam has two direct friends, Billy and Cindy. Between Adam and these two represents the shortest path length distance in the social network, so Adam is likely to mimic the behaviors of Billy or Cindy, or even both. Comparatively, Fred is not a direct friend of Adam, but knows of him through Eric, who knows Cindy. In this example, the distance between Adam and Fred

represents the longest path in the social network. Therefore, Adam is not as likely to be affected by the social behaviors of Fred as he would Cindy or Billy.

The contagion effect applies to more than just simple behaviors online, the effect helps explain why previously fair players can become cheaters on a gaming environment. (Canossa et al., 2019; Woo et al., 2018). These findings serve as an explanation of how cheating can travel through a social network of cheating players. In summary, not only can cheaters influence the likelihood of fair players to engage in cheating behaviors online, but the shorter social proximity between the two individuals will increase the magnitude of the relationship.

Thus, we propose the following hypotheses:

- H1- Cheating behavior is more prevalent in social networks with a known cheater compared to social networks without a known cheater.
- H2- Players who have cheaters in their immediate social network (i.e., friends) are more likely to cheat than players who have cheaters in their extended social network (i.e., friends of friends).
- H3- The number of banned players in a social network is positively related to the likelihood of cheating behavior among non-banned players in the same network.
- H4- There is a positive relationship between unity and cheating behavior. The greater the unity, the greater the likelihood an individual is cheating.
- H5- There is a positive relationship between unity and cheating behavior. The greater the social proof, the greater the likelihood an individual is cheating.

The first three hypotheses function as validation, first confirming the network effects as observed by Blackburn 2014 and extending the findings through the contagion effect. The last two hypotheses function as the theory explaining through what social mechanism the behavior spreads.


METHODOLOGY

To collect information on players' social networks, the platform to be used for this study is Steam. Data collection will be done on the VACLIST site to track accounts that were banned by the STEAM VAC ban. For an account to be included in our dataset, the account had to both be older than 6 months old and at least Steam level 5. We chose 6 months as younger accounts would not have a robust social network. We chose to exclude any accounts less than level 5 because levels are tied to games played, therefore an account at level 5 is considered too new, inactive, or not a real account. On the ban date, we manually identified: the account's STEAMID, type of ban, friends to the account at the time of ban, and the number of games banned. Below is an image example of the information to be obtained from VACLIST in Figure 1.

Once a user is identified, we review the summary profile to verify the number of bans, the type of ban, how many bans the user has experienced, and when the latest ban occurred. Only user profiles identified as public will be used for the dataset. The site also provides a link to the official Steam account profile where their friend network is visible. From the friend network we then identify all individuals who continue to be friends with the user on their social network at the time of banning as shown in Figure 2.

https://vaclist.net/account/76561198213859219

VacList stats about 76561198974660293



crypter
<https://steamcommunity.com/id/bfp93/>

Status: Public
 Created: 08/21/2015 almost 5 years ago

SteamID 64: 76561198213859219
 SteamID v3: [U:1:253593491]
 SteamID v1: STEAM_0:1:126796745

Game Ban: 2 game bans on record
 VAC Ban: 2 VAC bans on record
 Economy Ban: none
 Last Ban: 08/14/2020 3 days ago

Last Checked: 08/16/2020 about 23 hours ago

Figure 1 Information from VacList

crypter

FRIENDS 66

ALL FRIENDS Search friends by name or game

PLAYING

76561198136895272
 Counter-Strike: Global Offensive

ONLINE

ABDI	Cora	DGod
draft	field	jk
Ozzle	prigv	Strix

OFFLINE

\$	- sens	666
27463829273	:)	Alushi
Biebic	Bong-N-Bubbles	Bork Gates
BShow	CarrieLinderman	cheesy

Figure 2 Sample User Friendlist from Steam

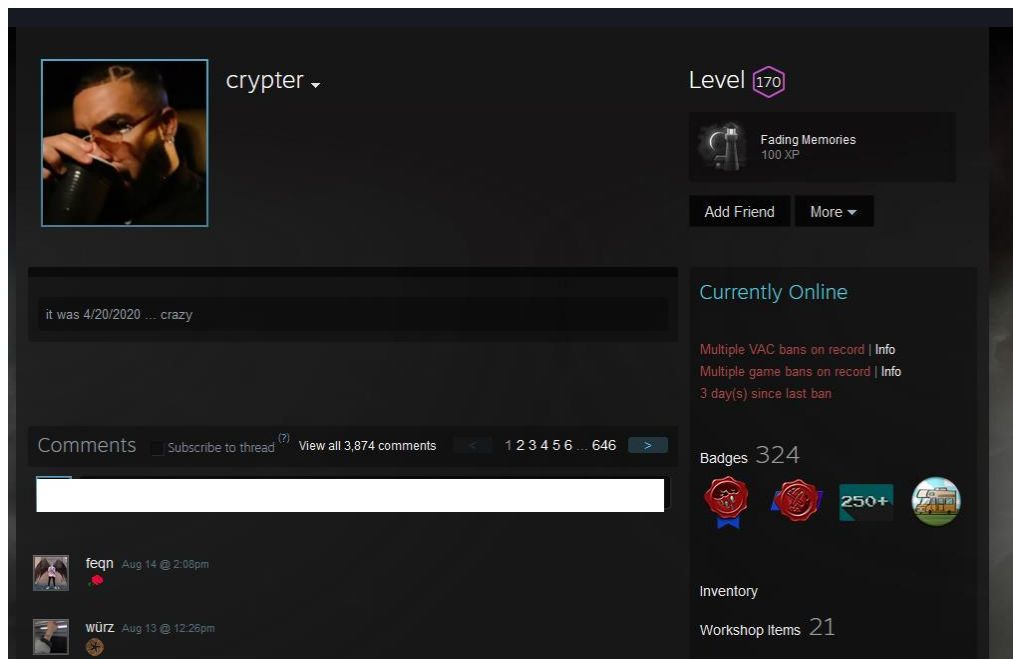


Figure 3 Sample Steam User Profile

The moment we identify and confirm a qualifying user network, we will begin to collect data using a data-scraping program written using Python language. As per Blackburn et al., immediate data collection from identification is important as we expect much of the social network changes to occur within the first few weeks. Furthermore, as Vaclist only reveals accounts as they are banned, we will limit data collection based on a window time frame. Our initial search and filtering will be run to collect all viable accounts over a month period. Data collection will be scraped from the Steam site linked on Vaclist. Our data categories will consist of profile descriptors such as the username, location, profile description, number of bans, time of banning, type of banning, games played, hours played per game, most frequently played games, player level, profile comments, and existing friend list. This information will be recorded in Database 1. A second database will consist of cross-referencing the STEAMID of the initial banned account with those on their friend's list. The list of friends is then recorded along with the repeating information categories scraped from the original, their own STEAM IDS, and their own friends are added to the database. This process

is then repeated twice more, with the friends of friends, and then the friends of friends of friends, establishing the social network depth of $N+3$. We anticipate a collection period of a week to two weeks to collect the necessary network information and will begin data collection in Mid-March. Finally, once the initial collection period is over, we will follow each source account and rerun the collection process weekly to detect changes in the social network. This process will continue for up to 3 months, or until we no longer detect any alterations in the network. In total, we anticipate a total data collection period of approximately 4 months. After data collection, we will model the friendship networks through a diagram to examine the relationships between cheaters and their friends. The goal is to develop a social network web of users and cheaters. The web will be used to identify clusters of cheaters in proximity to one another. For example, if subject B has been banned for cheating and has 6 friends on his network. Of those 6, 3 of them were banned for cheating and the other 3 were not. Among those 3 who were banned, they may be friends with one another, or friends with another cheater, or share similarities to subject B. Consider the following example scenario: Subjects X, I, E, J, A, and C, are each a member of their own social groups labeled groups 1-4. Assume each group has a direct path to their respective members. Subject B has been banned and has two individuals in his network that are non-outed cheaters, subjects X and I. From X's social network, we can see that he is close friends with subjects Z, O, L, and N, all of whom are not cheaters. This represents his immediate social circle. However, while not a close part of his personal social network, X is directly connected to E, J, and I who themselves are unknown cheaters. From the entire mapping of all groups 1-4 we can see a hidden group 5 exists between them that are all cheaters, even though some members are not even aware of each other. It is my aim to capture this network within networks.

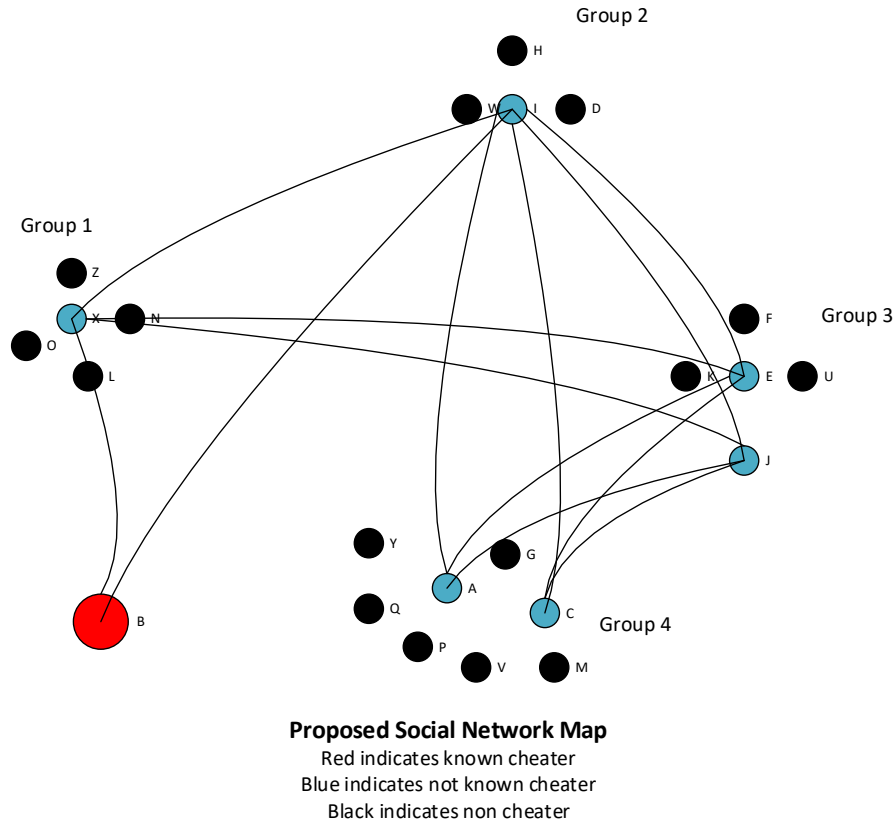


Figure 4 Proposed Social Network Map Scenario Example

Next, the cheater profile from database 1 will be run against the network map on database 2 to potentially develop an SEM model to predict if specific individuals are flagged for potential cheating behavior.

To test hypothesis 1, we will use the dataset collected from the gaming platform Steam, which includes user profiles and their gaming activity. We will first identify users who have been banned for cheating using the VAC system and extract their friend lists. These users will serve as the "known cheaters" in our study. We will then randomly select a control group of users from these friend lists who have not been banned for cheating and extract their friend lists as well. This control group will serve as the "social network without a known cheater" in our study.

Next, we will compare the proportion of users who have been banned for cheating in the social networks with a known cheater to the proportion of users who have been banned for cheating in the social networks without a known cheater. We will use a chi-square test to determine if the difference in proportions is statistically significant. If the proportion of cheaters is significantly higher in social networks with a known cheater compared to social networks without a known cheater, we will reject the null hypothesis and conclude that cheating behavior is more prevalent in social networks with a known cheater.

Hypothesis 2, Contagion theory suggests that the behavior of one's social network can influence an individual's own behavior. In the context of online gaming, it is possible that the presence of a cheater in one's social network can influence the likelihood of an individual being reported for cheating. If an individual sees their friends cheating and getting away with it, they may be more likely to engage in cheating behavior themselves. On the other hand, if an individual sees their friends being banned for cheating, they may be deterred from engaging in such behavior.

Sample Selection: The sample will consist of players who have a ban history for cheating and their friends on the gaming platform. To ensure that the sample is representative, a random sampling method will be used to select players who have been banned for cheating. Their friends on the platform will be identified using the existing friend list in the player's profile.

Data Analysis: A logistic regression analysis will be conducted to test the hypothesis. The dependent variable will be whether the player was banned for cheating, and the independent variable will be whether the player has a known cheater in their social network. Other control variables, such as player level and the number of hours played per week, will also be included in the analysis.

Expected Results: If the presence of a known cheater in a player's social network is positively associated with the likelihood of that player being reported for cheating, we would expect to see a significant positive coefficient for the independent variable in the logistic regression analysis, even after controlling for other factors. This would provide support for the hypothesis that the behavior of an individual's social network can influence their own behavior in the context of online gaming.

Hypothesis 3 extends the previous analysis and suggests that the number of banned players in a social network will increase the likelihood of cheating behavior among non-banned players in the same network. To test this hypothesis, we will use the data collected from the Steam platform, as described above.

First, we will identify the banned players in our sample and their social network connections. Then, we will compare the proportion of non-banned players who cheat in networks with a high number of banned players versus networks with a low number of banned players. We will use logistic regression analysis to determine the effect of the number of banned players on the likelihood of cheating behavior among non-banned players, while controlling for other relevant factors such as the size of the social network and the time spent playing the game.

We will operationalize cheating behavior as any violation of the Steam subscriber agreement related to gameplay, such as using third-party software to gain an unfair advantage or exploiting game glitches. We will use the same approach as in Hypotheses 1-3 to identify cheating behavior among non-banned players.

If our results show that the number of banned players in a social network is positively related to the likelihood of cheating behavior among non-banned players in the same network, we can conclude that this hypothesis is supported. We can also examine whether this effect is stronger for

certain types of games or certain characteristics of the social network, such as the density of connections between players.

Hypothesis 4: Unity, defined as the sense of connectedness and social identification with a group, has been found to be a predictor of individual behavior in a variety of contexts. In the context of gaming, individuals who play with others they perceive to be part of their social network may be more likely to conform to social norms established by the group, including the acceptability of cheating behavior. Thus, it is hypothesized that higher levels of unity will be positively associated with a greater likelihood of cheating behavior.

To test this hypothesis, data will be collected from gaming platforms that include information on individual cheating behavior as well as the social networks of the players. For this analysis, we will define unity as identifiers the player shares with others in their social network, such as location, frequency of communication, and time spent playing the same games. Social network analysis will be used to measure the level of unity within each social network. Logistic regression analysis will be conducted to determine whether there is a significant relationship between unity and cheating behavior, controlling for other relevant variables such as age, gender, and game type.

Hypothesis 5: Social proof refers to the concept that individuals are more likely to conform to behavior if they see others around them doing the same thing. In the context of gaming, this could mean that an individual is more likely to cheat if they see other players in their social network doing the same.

To test hypothesis 5, we will conduct a policy capture study using surveyed users on Amazon Mturk who have played Steam games. A control group of randomly selected individuals will be questioned on whether they would be willing to cheat. Then a second randomly selected sample

of participants will be given comparative scenarios which measure their willingness to engage in cheating behavior, manipulating how many individuals in their social network have cheated and for how long without being caught.

Finally, we will use regression analysis to examine the relationship between social proof and cheating behavior, while controlling for relevant demographic and gaming-related variables. If the results of our analysis indicate a significant positive relationship between social proof and cheating behavior, this would provide evidence in support of our hypothesis. Conversely, if the relationship between social proof and cheating behavior is found to be insignificant or negative, this would suggest that social proof may not be a significant factor in explaining cheating behavior in online gaming environments.

The results of this study would contribute to the understanding of the role of social influence in cheating behavior among online gamers. It would also provide insights into the importance of considering both unity and social proofing as potential factors that shape individuals' attitudes toward cheating in online gaming environments.

DISCUSSION

In existing cybersecurity literature, it is rare to obtain data on breaches and cyber-attacks that can be narrowed down to an individual person. Normally companies are loath to reveal this information as it represents a threat to the corporate shareholder value. Thus, utilizing Steam, data provides a rare opportunity to not only find positively identified cybercrime in the form of cheaters, but also to observe their peer's social network changes in real time. In current literature there is no known agreed upon method to actively predict the likelihood that an individual will engage in cheating behavior. While the literature has alluded to the possibility of such a circumstance by suggesting a greater likelihood of cheaters having friends who are cheaters, this research contributes to the

literature by both validating the original study, and proposing a method to apply a probability that an individual within a social network is engaged in cheating behavior. Furthermore, this research contributes to the broader literature of cybersecurity by proposing a potential method to identify and penetrate hidden networks of cyber vandals online by identifying higher risk social networks of cheating individuals.

Due to the nature of the available data there will be a few limitations to our research. First the dataset is limited to only users with publicly available information. This will lead to some degree of bias on the dataset as users with profiles set to private may have driving characteristics that may influence the results. However, this can be somewhat remedied if we can catch when individuals transition from public to private. If possible, future research into private accounts may allow for a comparison of results. The data will also be obtained through the Steam platform opening the possibility that the userbase population may have characteristics that are not shared with the users of other platforms. Future research can be done on other potential platforms where users experience similar bans such as Riot games or Blizzard's Battle.Net network.

Additionally, while applicable to other fields, one should be wary to apply these findings outside of the gaming domain. The research is intended to be on gaming social networks, and while there is overlap between cheating actions and cyber threats, the environment of other computer mediated fields may impact results. Further research can be done to extend this study into fields where organizational networks exist such as online academics, cyber theft, cybersecurity, or network enabled industry.

Finally, our dataset will not specifically list how the cheater got his ban, only what system caught him. Therefore, if there is a distinction between methods of cheating that could impact results, it would not be caught in this model and represents a further area of research.

CONCLUSION

Rampant cheating behavior is a significant problem in online gaming. The metaphorical arms race between developers and cheaters perpetually puts developers on the back foot. Yet with cheating's contagion like effect, it can be leveraged to predict the likelihood that someone would engage in cheating behavior. In the same way an individual tends to associate with likeminded others, human online social relationships behave the same way. If we can successfully identify the possibility of a person being a cheater, just in the practical sense, businesses and game developers can reduce losses caused by unethical players, by stamping out the contagion early. Even at the bare minimum, if it is possible to identify high risk factors it will allow security resources to be more efficiently utilized in cheating detection. Our model could function as a benchmark to identify illicit networks outside of the gaming environment where such social contagions occur as well, providing us with a tool to potentially penetrate social networks of cyber criminals allowing for agents to engage in preventative measures rather than responsive ones.

REFERENCES

- Ahmed Madhurja, S. S. 2020. "Our negligence of the ever-growing gaming industry," *The Daily Star*, March 3 (available at <https://www.thedailystar.net/opinion/news/our-negligence-the-ever-growing-gaming-industry-1875901>; retrieved May 2, 2023).
- Amblee, N., and Bui, T. 2011. "Harnessing the influence of social proof in online shopping: The effect of electronic word of mouth on sales of Digital Microproducts," *International Journal of Electronic Commerce* (16:2), pp. 91–114 (doi: 10.2753/jec1086-4415160205).
- Bandura, A. (1999) "Social Cognitive Theory: An agentic perspective," *Asian Journal of Social Psychology*, 2(1), pp. 21–41. Available at: <https://doi.org/10.1111/1467-839x.00024>.
- Blackburn, J., Kourtellis, N., Skvoretz, J., Ripeanu, M., and Iamnitchi, A. 2014. "Cheating in online games," *ACM Transactions on Internet Technology* (13:3), pp. 1–25 (doi: 10.1145/2602570).
- Blackburn, J., Simha, R., Kourtellis, N., Zuo, X., Ripeanu, M., Skvoretz, J., and Iamnitchi, A. 2012. "Branded with a scarlet 'C,'" *Proceedings of the 21st international conference on World Wide Web* (doi: 10.1145/2187836.2187848).
- Braca, A., and Dondio, P. 2023. "Persuasive communication systems: A machine learning approach to predict the effect of linguistic styles and persuasion techniques," *Journal of Systems and Information Technology* (doi: 10.1108/jsit-07-2022-0166).
- Canossa, A., Azadvar, A., Harteveld, C., Drachen, A., and Deterding, S. 2019. "Influencers in multiplayer online shooters," *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (doi: 10.1145/3290605.3300489).
- Christakis, N. A., and Fowler, J. H. 2012. "Social contagion theory: Examining dynamic social networks and human behavior," *Statistics in Medicine* (32:4), pp. 556–577 (doi: 10.1002/sim.5408).
- Christensen, J., Cusick, M., Villanes, A., Veryovka, O., Watson, B., & Rappa, M. (2013). *Win, Lose or Cheat: The Analytics of Player Behaviors in Online Games*. 7.
- Cialdini, R. B. (2008). *Influence* (5th ed.). Pearson.
- Cialdini, R. B. 2018. *Pre-suasion: A revolutionary way to influence and persuade*, New York: Simon & Schuster Paperbacks.
- Contractor, N. S., and DeChurch, L. A. 2014. "Integrating social networks and human social motives to achieve social influence at scale," *Proceedings of the National Academy of Sciences* (111:supplement_4), pp. 13650–13657 (doi: 10.1073/pnas.1401211111).
- Eskine, K. J., Novreske, A., and Richards, M. 2013. "Moral contagion effects in everyday interpersonal encounters," *Journal of Experimental Social Psychology* (49:5), pp. 947–950 (doi: 10.1016/j.jesp.2013.04.009).
- Fabrega, J., and Paredes, P. 2013. "Social Contagion and cascade behaviors on Twitter," *Information* (4:2), pp. 171–181 (doi: 10.3390/info4020171).
- Frostling-Henningsson, M. 2009. "First-person shooter games as a way of connecting to people: 'Brothers in blood,'" *CyberPsychology & Behavior* (12:5), pp. 557–562 (doi: 10.1089/cpb.2008.0345).
- Holpuch, A. 2022. "Gaming is booming. that's catnip for cybercriminals.," *The New York Times*, The New York Times, October 13 (available at <https://www.nytimes.com/2022/10/13/technology/gamers-malware-minecraft-roblox.html>; retrieved May 1, 2023).

- Kappler, K. 2018. "Hill/Dunbar (2003): Social network size in humans," *Schlüsselwerke der Netzwerkforschung*, pp. 263–265 (doi: 10.1007/978-3-658-21742-6_60).
- Jeff Yan, J., and Choi, H. J. 2002. "Security issues in online games," *The Electronic Library* (20:2), pp. 125–133 (doi: 10.1108/02640470210424455).
- Klumpe, J., Koch, O. F., and Benlian, A. 2018. "How pull vs. Push Information Delivery and social proof affect information disclosure in location based services," *Electronic Markets* (30:3), pp. 569–586 (doi: 10.1007/s12525-018-0318-1).
- Krause, J., Croft, D. P., and James, R. 2007. "Social network theory in the behavioural sciences: Potential applications," *Behavioral Ecology and Sociobiology* (62:1), pp. 15–27 (doi: 10.1007/s00265-007-0445-8).
- Ladanyi, J., and Doyle-Portillo, S. 2017. "The development and validation of the grief play scale (GPS) in mmorpgs," *Personality and Individual Differences* (114), pp. 125–133 (doi: 10.1016/j.paid.2017.03.062).
- Liao, G.-Y., Tseng, F.-C., Cheng, T. C. E., and Teng, C.-I. 2020. "Impact of gaming habits on motivation to attain gaming goals, perceived price fairness, and online gamer loyalty: Perspective of consistency principle," *Telematics and Informatics* (49), p. 101367 (doi: 10.1016/j.tele.2020.101367).
- Nacos, B. L. 2009. "Revisiting the contagion hypothesis: Terrorism, news coverage, and copycat attacks," (available at <http://www.jstor.org/stable/10.2307/26298412?refreqid=search-gateway>).
- Neto, H. C., Carvalho, L. F., Paraguaçu, F., and Lopes, R. V. 2011. "A MMORPG decision-making model based on persuasive reciprocity," *Lecture Notes in Computer Science*, pp. 33–47 (doi: 10.1007/978-3-642-24918-1_7).
- Petty, R. E., Cacioppo, J. T., and Abraham, C. 1986. *The elaboration likelihood model of persuasion*.
- Press Release by Chino May 2nd, 2018 07:56 D. (30 C. 2018. "Widespread cheating in multiplayer online games frustrates consumers," *TechPowerUp*, May 2 (available at <https://www.techpowerup.com/243832/widespread-cheating-in-multiplayer-online-games-frustrates-consumers>; retrieved May 4, 2023).
- Posey, C., Lowry, P. B., Roberts, T. L., and Ellis, T. S. 2010. "Proposing the online community self-disclosure model: The case of working professionals in France and the U.K. who use online communities," *European Journal of Information Systems* (19:2), pp. 181–195 (doi: 10.1057/ejis.2010.15).
- Reicher, S. D., Spears, R., and Postmes, T. 1995. "A social identity model of deindividuation phenomena," *European Review of Social Psychology* (6:1), pp. 161–198 (doi: 10.1080/14792779443000049).
- Roethke, K., Klumpe, J., Adam, M., and Benlian, A. 2020. "Social influence tactics in e-commerce onboarding: The role of social proof and reciprocity in affecting user registrations," *Decision Support Systems* (131), p. 113268 (doi: 10.1016/j.dss.2020.113268).
- Saarinen. (2017, November 5). "Toxic behavior in online games - Oulu," (available at <http://jultika.oulu.fi/files/nbnfioulu-201706022379.pdf>; retrieved February 4, 2023).
- Scherer, C. W., and Cho, H. 2003. "A social network contagion theory of risk perception," *Risk Analysis* (23:2), pp. 261–267 (doi: 10.1111/1539-6924.00306).
- Schunk, D. H., and Zimmerman, B. J. 1997. "Social origins of self-regulatory competence," *Educational Psychologist* (32:4), pp. 195–208 (doi: 10.1207/s15326985ep3204_1).

- Scott, J. 1988. "Social network analysis," *Sociology* (22:1), pp. 109–127 (doi: 10.1177/0038038588022001007).
- Sheldon, M. D., Bhattacharjee, S., and Barkhi, R. 2023. "The impact of persuasive response sequence and consistency when Information Technology Service Providers Address Auditor-identified issues in system and organization Control 2 Reports," *Journal of Information Systems* (37:1), pp. 85–107 (doi: 10.2308/isis-2021-016).
- Shih, H.-P., Lai, K.-hung, and Cheng, T. C. 2023. "Complied by belief consistency: The cognitive-information lens of user-generated persuasion," *Journal of Theoretical and Applied Electronic Commerce Research* (18:1), pp. 372–393 (doi: 10.3390/jtaer18010020).
- Teng, S., Khong, K. W., Chong, A. Y., and Lin, B. 2016. "Persuasive electronic word-of-mouth messages in social media," *Journal of Computer Information Systems* (57:1), pp. 76–88 (doi: 10.1080/08874417.2016.1181501).
- Vargheese, J. P., Collinson, M., and Masthoff, J. 2020. "Exploring susceptibility measures to persuasion," *Lecture Notes in Computer Science*, pp. 16–29 (doi: 10.1007/978-3-030-45712-9_2).
- Vargheese, J. P., Collinson, M., and Masthoff, J. 2022. "A quantitative field study of a persuasive security technology in the Wild," *Lecture Notes in Computer Science*, pp. 211–232 (doi: 10.1007/978-3-031-19097-1_13).
- "Video games - worldwide: Statista market forecast." (n.d.). Statista (available at <https://www.statista.com/outlook/dmo/digital-media/video-games/worldwide>; retrieved January 25, 2023).
- Wang, L., Fan, L., and Bae, S. M. 2019. "How to persuade an online gamer to give up cheating? uniting elaboration likelihood model and signaling theory," *Computers in Human Behavior* (96), pp. 149–162 (doi: 10.1016/j.chb.2019.02.024).
- Woo, J., Kang, S. W., Kim, H. K., and Park, J. 2018. "Contagion of cheating behaviors in online social networks," *IEEE Access* (6), pp. 29098–29108 (doi: 10.1109/access.2018.2834220).
- Wu, Y., and Chen, V. H. 2013. "A social-cognitive approach to online game cheating," *Computers in Human Behavior* (29:6), pp. 2557–2567 (doi: 10.1016/j.chb.2013.06.032).
- Wu, Y., and Chen, V. H. 2018. "Understanding online game cheating: Unpacking the ethical dimension," *International Journal of Human–Computer Interaction* (34:8), pp. 786–797 (doi: 10.1080/10447318.2018.1461757).
- Yan, J., and Randell, B. 2005. "A systematic classification of cheating in online games," *Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games* (doi: 10.1145/1103599.1103606).
- Yuen, K. F., Tan, L. S., Wong, Y. D., and Wang, X. 2022. "Social Determinants of panic buying behaviour amidst COVID-19 pandemic: The role of perceived scarcity and anticipated regret," *Journal of Retailing and Consumer Services* (66), p. 102948 (doi: 10.1016/j.jretconser.2022.102948).
- Zhao, Z., Calderón, J. P., Xu, C., Zhao, G., Fenn, D., Sornette, D., Crane, R., Hui, P. M., and Johnson, N. F. 2010. "Effect of social group dynamics on contagion," *Physical Review E* (81:5) (doi: 10.1103/physreve.81.056107).
- Zuo, X., Gandy, C., Skvoretz, J., and Iamnitchi, A. 2021. "Bad apples spoil the fun: Quantifying cheating in online gaming," *Proceedings of the International AAAI Conference on Web and Social Media* (10:1), pp. 496–505 (doi: 10.1609/icwsm.v10i1.14745).