2009

The Economy Of Cheating In Mmorpgs: A Case Study Of Innovation

Stefano De Paoli
National University of Ireland Maynooth, Stefano.DePaoli@nuim.ie

Aphra Kerr
National University of Ireland Maynooth, Aphra.Kerr@nuim.ie

THE ECONOMY OF CHEATING IN MMORPGS: A CASE STUDY OF INNOVATION

De Paoli, Stefano, National University of Ireland Maynooth, Maynooth, Co. Kildare, Rep. of Ireland, Stefano.DePaoli@nuim.ie
Kerr, Aphra, National University of Ireland Maynooth, Maynooth, Co. Kildare, Rep. of Ireland, Aphra.Kerr@nuim.ie

Abstract

Massive Multiplayer Online Role-Playing Games are socio-technical phenomena that are both complex technological systems and complex societies. They are also highly lucrative businesses. In this paper we present initial findings from a case study of the MMORPG TIBIA which explores the business and social relationships generated by cheating practices. We characterize the economy of cheating as a learning and innovation process and the development of cheating solutions as an answer to breakdowns and market demand.

Keywords: *Economy of Cheating, Mmorpg, Emergent Approach, Breakdown, Innovation, Learning*

1 INTRODUCTION

Massive Multiplayer Online Role-Playing Games (MMORPGs) are a highly successful sub-sector of the digital games industry whereby players pay monthly subscriptions to participate in a virtual world which is persistent, meaning that it runs independently from the user, and requires continuous customer support from the game developer (Kerr, 2006). They are both highly sophisticated technological systems, in most cases built around a client-server architecture and 'deeply social' (Taylor, 2006) worlds where millions of players chat, cooperate, interact, compete and trade with each other online through their avatars.

In our research we are concerned with trust and security issues in online worlds. Cheating in an MMORPG is a highly contested practice that deserves particular attention, insofar as it is perceived by the developers and publishers of MMORPGs to be a real threat to the social experience, economic viability and security of a game world. For others, cheating is more justifiable and the potential to generate real money, to enhance one's reputation or to win a game are motivations for both companies selling cheats and players willing to use those cheats.

In this paper we adopt an emergent approach to studying *how the economy of MMORPGs is influenced by cheating practices*. Focusing on the "how" we seek to provide an account (Garfinkel, 1967; Latour, 2005) of the phenomenon under scrutiny using qualitative research methods and we seek to avoid focusing our work just on the negative impact of cheating in MMORPGs, which might foreclose an understanding of the dynamics of this phenomenon. This paper is based on an ongoing case study of the MMORPG TIBIA, (http://www.tibia.com) and the struggle between its developer CipSoft and external companies to regulate and exploit cheating practices. It is a dynamic story of a relationship which involves processes of learning and incremental innovation of new software tools and policies to regulate player behaviour. The paper includes a brief review of relevant literature; a discussion of our methodology; examples of cheating, learning and innovation practices surrounding TIBIA and finally some concluding remarks.

2 CHEATING IN A NUTSHELL

According to the game theorist Huizinga (1955), cheating can be roughly described as something that is "*harmful for game play*" (p. 52). This relates to the common definition of cheating in online games as the set of *"activities that modify the game experience to give one player an advantage over another player(s);*" (Cheating in online games, 2009).

A lot of the technical literature on cheating defines it as something detrimental to gameplay and as a threat to be defeated. In this literature there is a dialectic between the diffusion of cheating and exploits techniques in online games (the thesis) and the need for powerful anti-cheating techniques (the antithesis). In this dialectic the desired final synthesis is to reach an idealistic state in which the game becomes fair (free of cheats) for everyone. In online games it is possible to recognize several different types of cheating, that vary according to different techniques and exploits (see Yan and Randell, 2005). Examples of anti-cheating techniques, include the use of captcha to detect "bot" users (Golle and Ducheneaut, 2007), anti-cheating protocols (Di Chen and Maheswaran, 2004), techniques for preventing software client modifications (Mönch et al., 2006), and techniques used to detect known cheats in real time games (Ferretti and Rocetti, 2006).

By contrast media scholars have pointed out that cheating is multidimensional and contested. For example Consalvo (2007) provides a rich conceptualization focused on how players negotiate what cheating actually is. Fields and Kafai (2007) describe the learning process thorough which cheats for online games are created. Kücklich (2007) has proposed to use cheating as a possible methodology to explore non-obvious aspects of the gameplay.

3 AN EMERGENT APPROACH

In studying the economy of cheating we do not seek to test a hypothesis or a formal model, nor are we interested in the motivations of (cheating) companies and (cheating) players. We adopt an emergent approach that seeks to account for the socio-technical process related to the economy of cheating. In particular we emphasize the accounts that are directly provided by the actors we are studying: how the various cheating companies account for their business, and how the customers of these companies see the services and products that are being offered. In doing so we follow an important tradition in IS research related to phenomenology (see in particular Ciborra, 2002; Winograd and Flores, 1987; Latour 1987, 2005). In particular we adopt the principle whereby the observer does not decide in advance the attributions of social and technical elements of the system. Instead, using "*Ethno*"-"*methods*" (Garfinkel, 1967) we allow the attributions to emerge from the negotiations surrounding the system.

One of the key elements for approaching IS practices and their social and technical attributes is to focus on the moments of rupture from the "natural flow of things". Akrich (1992) observed that we need to focus on disputes around technology or situations in which devices go wrong, as the crucial moments that reveal the negotiations surrounding the design, development and use of technologies. In a similar vein Winograd and Flores (1987) proposed the concept of breakdown. In this paper we study the economy of cheating as a situated practice that might reveal its characteristics in the disputes or breakdowns around technological and social aspects of cheating practices.

The role of users in the innovation process is a focus for researchers from evolutionary economics, to science and technology studies to media studies (Edquist, 1997; Haddon & Paul, 2001; van Oost, et al., 2009). Users can have indirect (through market research) or more direct roles (through testing and participatory design) roles in the innovation process and their tacit and lay knowledge can provide important inputs to the innovation process. In this paper we consider innovation to be a dynamic process which can be either radical or incremental and which leads to the development of a

new product or process, including new regulatory policies, in the marketplace. Innovation is a collaborative process of learning and knowledge development which increasingly takes place in networks, rather than purely internally in companies, and which involve a range of human and non-human actors, from users/players, to firms and to technologies.

The data in this paper draws upon ongoing ethnographic observations (Hine, 2000) of the official TIBIA forums and the forums of cheating companies. In particular we have devoted our attention to forum posts directly related with an anti-cheating campaign by the game developer. These posts have been collected using the archiving software Scrapbook. In term of data analysis our strategy is very close to that proposed by Latour (1988, p. 10) that suggests one follow the "storytellers" (i.e. the main actors) and how they attribute causes, endow entities with qualities or classify actors without trying to impose a predetermined grid of analysis.

4 THE CASE OF TIBIA AND THE CHEATING COMPANIES

TIBIA is a 2D medieval and fantasy MMORPG that was first released in 1997. TIBIA is played on more than 70 servers located in Germany and the USA, with an estimated subscriber base of 300,000 players (120000 are premium accounts) (CipSoft, 2009). TIBIA was chosen for this case study of the phenomenon of cheating because CipSoft, the company that develops and distributes the game, started a campaign against cheaters at the beginning of 2009.

In TIBIA cheaters, especially "botters" are widespread on all the game servers. "Botting" is the practice by which a player uses an external computer program to automate certain gameplay tasks. As in many other MMORPGs, TIBIA players must perform certain actions such as killing and looting monsters in order to acquire special items and virtual currency and bots can assist or replace the players in performing these tasks. Two companies in particular, "BlackD" and "NGSoft", are well known to TIBIA players for providing "bots" and they sell licenses for their bot programs in exactly the same way as any commercial software company does.

The ongoing anti-cheating campaign by CipSoft against cheaters and bots has included mass bans, new anti-cheating tools and changes to the game's regulatory policies. In this regard one of the most talked about moves was the introduction of an anti-cheating tool. Anti-cheating tools are software devices that automatically enforce the rules contained in the End User License Agreement or the Terms of Service rules. Anti-cheating tools also pursue the use of third party software (such as bots) that tampers with software clients. One of the mass bans (02 April 2009) operated by the company was announced on their forums as: "*Today, 5103 Tibia accounts have been punished for using unofficial software to play during the last weeks. These accounts have been identified by our automatic tool."*. In this message CipSoft claims that the ban action was undertaken on the basis of information gathered by an anti-cheating tool.

The automatic anti-cheating tool clearly interferes both with the behaviour of cheaters and the business of the external cheating companies. Indeed, the campaign against cheating and the introduction of the anti-cheating tool is an element that changes the actual configuration of the situation: it is a real moment of breakdown for cheating companies. Before the current anti-cheating campaign, it was common knowledge that using bots in TIBIA was easy. On the official game forums several "fair" players, in different threads, described the domination of botters on game servers and hunting areas. On the cheating forums meanwhile cheaters share images or even videos of cheating "projects" (i.e. the creation of powerful characters leveled by using bots). The introduction of the anti-cheating tool has, however, radically modified the situation for cheating companies and cheaters. Interestingly, this breakdown has also lead cheating companies to declare their aimbition to develop a new detection-safe version of their bot and signals a new process of learning and innovation involving cheaters and the cheating companies.

4.1 Cheating as supply and demand relationship

CipSoft made the first mass ban at the beginning of February 2009, one month after the publication on their website of an article on their anti-cheating strategy. This mass ban was unexpected by fair players, cheating players and cheating companies. And in fact many fair players have described the ban as a good starting point in the campaign against TIBIA cheaters. By contrast for cheating companies the mass ban constitute a serious threat to the cheating business, while cheaters have described the new situation as "the end of botting". After the mass ban many bot customers were afraid to use these cheating programs while playing TIBIA. What follows is a poll that was launched on one of the cheating forums after the first mass ban, which asked "*Are you botting?*".

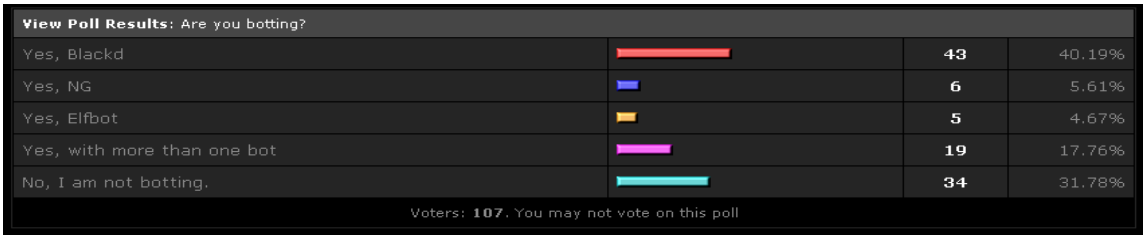

Figure 1 Poll on BlackD forum on the use of bot
http://www.blackdtools.com/forum/showthread.php?t=36002

Although this poll does not have statistical validity, it shows (in the last line) that almost one third of respondents (34/107) declared their intention to stop using bots. In a way the poll shows the mood of some customers, and their decision to stop using bots. The introduction of the anti-cheating tool has changed the relationship between cheating companies, the cheating software and cheating players: botting went from being a safe and rarely punished activity to a very dangerous activity, with a high risk of being banned. It is clear that the customers' intention to stop using bots is a serious potential business problem for cheating companies and could lead to a possible decrease in the demand for bots and consequently a decrease in revenues.

4.2 Cheating as a learning process – player/firm interactions

One of the key issues is that the cheating companies do not know how the CipSoft anti-cheating detection system operates, and this creates a problem for the development of new undetectable bots that can provide customers with the necessary guarantee to be safe from bans. This is of course not just an accident, but it is clearly part of the CipSoft strategy, as the following message by a TIBIA community manager shows:

Concerning the speculations and rumours about our automatic tool:
We won't comment on all those speculations since any hint would only help cheat tool developers and cheaters. Likewise, we won't reveal or discuss our criteria.

(From http://forum.tibia.com/forum/?action=thread&threadid=2478964&pagenumber=29 Post #22067302, 02/02/2009)

So, as a general strategy against cheating companies, CipSoft does not want to reveal anything about the anti-cheating tool. Therefore, for cheating companies, in order to meet the new customers' demand for undetectable bots it becomes essential to acquire some knowledge on how the anti-cheating tool works. Fields and Kafai (2007) describe how cheating in online games is often a learning process in which cheaters collectively learn how to use cheats. In the case of TIBIA, CipSoft, the cheating companies and players are involved in a learning process and there is a clear relationship between cheating and learning. We have a process through which real software companies, helped by cheating players, try to learn how an anti-cheating tool works. The goal of the learning process is

to develop a way to defeat a cheating countermeasure. On the TIBIA cheating forums this learning process is pursued by inferring the behaviour of the game client (after the tool introduction), based on the companies and cheaters knowledge of computer systems. What follows is a forum post by the cheating company BlackD that describes what the company owner calls a possible "theory" on how the anti-cheating tool works:

THEORY 1: […]

My guess is Tibia client can obtain the list of your installed programs, and it can send the list to tibia servers, probably only on request, when a scan wave happens, maybe only once each month (because it causes big lag, kicks and deaths for everybody) If tibia client sended that always at start then it would bee too easy to catch that packet.

I will appreciate help from people who can read hex, and know about the API who can obtain the list of installed programs. The call is probably somewhere in the code of the tibia client. That would confirm my theory

(From http://www.blackdtools.com/forum/showthread.php?t=35800, 01/30/09)

It is interesting to see how cheating is both a socio-technical process as well as a learning process, in which various technological elements (for example installed programs, API, call to functions) form cheating business practices. In this case BlackD guesses that the anti-cheating tool operates by searching well know strings (i.e. installation names) on the users' machines. As we can see, cheaters with technical knowledge (people who can read hex and know the API) are invited by the cheating company to contribute to this learning process and provide knowledge that can confirm/disconfirm this theory. What follows is an example of this learning process, with a cheater providing some hints as to the inner activities of the TIBIA client:

It is also possible that Cip changed some server packets (1 byte is enough I believe) and updated the client to use the new packets...so when the bot uses the old packet, account is logged and banned.

(From http://www.blackdtools.com/forum/showthread.php?t=35800&page=6, 01/30/2009)

Here we see how cheaters contribute to the learning process. In this example, the cheater assumes that the tool checks communication packets between the client and the server and that CipSoft has slightly changed some packets so that detecting the tampering activities of bots becomes easy. What follows is a second "theory" on the inner working functioning of the anti-cheating tool, again proposed by BlackD:

THEORY2:
they search strings "blackd" "ng" "elfbot" in your chat logs (private or not) If string is found more than 10 times in the log of the last 6 months then that would be "enough" proof and you get an automatic ban.

(From http://www.blackdtools.com/forum/showthread.php?t=35800, 01/30/09)

In this case the company proposes the idea that the anti-cheating tool scans the players' chat logs searching for known strings (e.g. "blackd") related to bots. The idea is that if a player has written certain strings several times in the chat while communicating with others, in a given period of time, then this is detected by the anti-cheating tool. The ban of cheaters will be based on checking this information. What follows is a comment by a cheater on a possible reason why this proposed second theory is not correct:

Theory two doesn't work because I have said such things thousands of times in Tibia and no banishment. (From http://www.blackdtools.com/forum/showthread.php?t=35800&page=5, 01/30/09)

In this case we have a positive guess based on the consideration that the cheater has used the strings several times in chat but he/she has not got banned. On the contrary what follows is a negative guess:

The second theory has to be false... I was banished but I didn't talk about bots ingame.

(From http://www.blackdtools.com/forum/showthread.php?t=35800&page=7, 01/30/09)

The second theory is therefore contradicted by the consideration that this cheater got banned even if he/she has never used those strings in chat.

The evidence gathered so far would lead us to agree with Fields and Kafai that cheating can be conceptualized as a learning process. However in our story, the focus of the learning process is not on playing and winning the game, but rather on learning how the anti-cheating tool functions.

4.3 Cheating as part of an Innovation Process

Cheating in TIBIA results in multiple innovations by a range of actors. CipSoft's anti-cheating campaign since January 09 has involved the introduction of two innovations: the anti-cheating tool and new governance policies. This has forced the cheating companies to start a process of "Research and Development" which is resulting in incremental product innovations to combat the anti-cheating tool. For the cheating firms the process involves them gathering information from players about their products in the marketplace and about competing technologies and subsequently using this information to assist in the development of new cheating technologies. Thus the cheating firms are not just involved in an information gathering and learning process, they are also involved in a highly iterative innovation process to develop new software products and maintain their business.

For cheating companies the innovation process is attempting to do two things: develop undetectable bots and to reassure their customers. The following message by NGSoft clearly aims to reassure those customers who have become afraid to use bots because of the mass bans and foresees the creation of a new generation of undetectable bots:

Our response instead will be to research and create a new type of undetectable bot that does not modify the Tibia client and therefore will be safe to use under all circumstances even if Tibia does implement a client-side bot detection routine. (From http://forums.tibiabot.com/showthread.php?t=110349, 02/01/2009)

In fact new versions of bots were released shortly after the first mass ban, incorporating several enhancements that were supposed to counteract the anti-cheating tool. These incremental innovations were based on the information provided by cheaters via public forums. Interestingly, the first mass ban has been followed by a second and a third. These subsequent bans constitute a dynamic situation in which the new bots were tested in the market place. On the cheating forums, cheaters were asked by the company to provide feedback on characters created after the first mass and leveled with the new bots. While many cheaters said that their newly created characters were not banned in this second wave, some were:

YES I GOT BANNED WITH ONE. Created AFTER the proxy improvements (From http://www.blackdtools.com/forum/showthread.php?t=37571, 03/03/2009).

At the beginning of March 2009 the company declared on its website that using the bot should be safe. However, at the beginning of April, after a third mass ban, the advice from the cheating companies changed, as the following message demonstrates:

Using any bot seems to be very risky nowadays until we know how bots are exactly detected. We keep investigating on this but we should recommend to avoid botting with main characters. (From http://www.blackdtools.com/news.php?p=2, 04/02/2009).

So far, therefore, the incremental technological innovations developed by the cheating companies do not appear to have generated the required result and cheaters are being advised to adopt gameplay solutions to cheat. No secure and undetectable bot has been created and the use of bots in TIBIA remains a very risky activity for cheaters. At the moment cheating companies appear to have lost their "fight" against the TIBIA anti-cheating tool and while they have been innovating and actively engaging with their users they may not succeed in the marketplace.

5 CONCLUSION: THE ECONOMY OF CHEATING

The goal of this paper was to explore how in game cheating behaviour generates innovations in the real world economy using an emergent approach. In the case of TIBIA what we have described is a clash between the business of MMORPG companies and the business of cheating companies with both innovating in response to demands from different groups of players which are communicated largely through public forums.

In this case study we have told how TIBIA cheating companies have faced a rupture in their business and how these companies have tried to cope with this breakdown and user demands. Interestingly this breakdown resembles a negative externality, in which the anti-cheating tool "externally" and "negatively" influence the existing market relationships between the cheating companies and their customers. As Callon (1999) pointed out, answering this kind of negative external influence requires a new configuration, a new framing, of the existing network of socio-technical relations. And indeed the breakdown introduced by the anti-cheating tool required cheating companies to shape new relationships among themselves, their customers and their products, in order to re-frame a certain "order of things". The reconfiguration, in particular, has involved a learning and innovation process aimed at acquiring knowledge on the functioning of the negative externality and creating a new marketable product as an answer to the negative externality.

In conclusion, from a research point of view it is clear that cheating in MMORPGs should not be regarded just as a problem, as most part of technical literature does. Cheating is a problem from the perspective of some actors, but mono-dimensional explanation are limited insofar they prevent us from observing other dynamics. In this case study we have unveiled how cheating can be productive in a very real sense and the socio-technical complexity of the relationship between cheating companies, their customers and TIBIA. Future research will be required in order to assess other dynamics of this phenomenon.

References

Akrich, M. (1992). The De-Scription of Technical Objects. In *Shaping Technology/ Building Society*, Bijker, W. & Law, J. (Eds.), Cambridge, Mass: MIT Press, pp. 205-224.

Callon, M. (1999). Actor network theory: the market test. *Actor Network Theory and After*, Law J. and Hassard J. (Eds, Oxford: Blackwell, pp. 181 – 195.

Ciborra, C. (2002). *The Labyrinths of Information.* Oxford: Oxford University Press.

CipSoft (2008). *Massive Multiplayer Online Game Server*. Presentation at QuoVadis Conference, Berlin 07 May, 2008, URL: http://www.cipsoft.com/files/QuoVadis-MMOGServer.ppt

CipSoft (2009). *Where Will Cheaters Go From Here?*.URL: http://www.tibia.com/news/?subtopic=latestnews&id=910

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

Di Chen, B. & Maheswaran, M. (2004). A cheat controlled protocol for centralized online multiplayer games. In *Proceedings of 3rd ACM SIGCOMM Workshop on Network and System Support For Games*. ACM, New York, NY, 139-143. URL: http://doi.acm.org/10.1145/1016540.1016554

Edquist, C. (Ed.). (1997). *Systems of innovations*. London: Pinter.

Ferretti, S. & Rocetti, M., (2006). AC/DC: an algorithm for cheating detection by cheating. In *Proceedings of the 2006 international workshop on Network and operating systems support for digital audio and video*. Newport, Rhode Island, Article No. 23 . URL: http://portal.acm.org/citation.cfm?id=1378191.1378220.

Fields, D.A. & Kafai, Y.B. (2007). Stealing from Grandma or Generating Cultural Knowledge? Contestations and Effects of Cheats in a Teen Virtual World. In *Situated Play, Proceedings of the DiGRA 2007*, URL: http://www.digra.org/dl/db/07312.48067.pdf

Garfinkel, H. (1967). *Studies in ethnomethodology* . Englewood Cliffs, NJ: Prentice-Hall.

Golle, P. & Ducheneaut, N. (2005). Preventing bots from playing online games. *Comput. Entertain.* 3, (3) (Jul. 2005). URL: http://doi.acm.org/10.1145/1077246.1077255

Haddon, L., & Paul, G. (2001). Design in the IT Industry: the role of users. In, *Technology and the Market. Demand, Users and Innovation,* Coombs R., Green K., Richards A. & Walsh V. (Eds.), Northampton: Edward Elgar Publishing Inc, pp. 201-215.

Hine, C. (2000). *Virtual Ethnography.* Sage Publications, Thousand Oaks.

Huizinga, J. (1955). *Homo ludens; a study of the play-element in culture*. Boston: Beacon Press.

Kerr, A. (2006). *The business and culture of digital games: gamework/gamplay*. London: Sage.

Kücklich, J., (2007). Home Deludens - Cheating as a methodological tool in digital game's Research. *Convergence*, 13(4), pp. 355-367.

Latour, B. (1987). *Science in Action.* Cambridge Mass.: Harvard University Press.

Latour, B.(1988). *The pasteurization of France.* Cambridge Mass.: Harvard University Press.

Latour, B. (2005). *Reassembling the Social*. Oxford: Oxford University Press.

Mönch, C., Grimen, G., & Midtstraum, R. (2006). Protecting online games against cheating. In *Proceedings of 5th ACM Workshop on Network and System Support For Games*. ACM, New York, NY, 20.

Taylor, T. L. (2006). *Play Between Worlds*. Cambridge, Mass.: The MIT Press.

van Oost, E., Verhaegh, S., & Oudshoorn, S. (2009). User-initiated Innovation in Wireless Leiden. From Innovation Community to Community Innovation. *Science, Technology and Human Values*, 34(182), pp. 182-205.

Winograd, T. & Flores, F. (1986). *Understanding Computer and Cognition*. Norwood, NJ: Ablex.

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