Journal of
Virtual Worlds Research
jvwresearch.org ISSN: 1941-8477

Virtual Economies, Virtual Goods and Service Delivery in Virtual Worlds

Volume 2, Number 4

Volume 2, Number 4
Virtual Economies, Virtual Goods and Service Delivery in Virtual Worlds
February 2010

The Journal of Virtual Worlds Research
is owned and published by the
Virtual Worlds Institute, Inc.
Austin, Texas, USA.

The Journal of Virtual Worlds Research is funded by its sponsors and contributions from readers. If this material is useful to you, please consider making a contribution. To make a contribution online, visit: http://jvwresearch.org/donate.html

Journal of Virtual Worlds Research
jvwresearch.org ISSN: 1941-8477

Volume 2, Number 4
Virtual Economies, Virtual Goods and Service Delivery in Virtual Worlds
February 2010

"We Will Always Be One Step Ahead of Them"

A Case Study on the Economy of Cheating in MMORPGs

By Stefano De Paoli and Aphra Kerr
Department of Sociology and NIRSA, National University of Ireland Maynooth

Abstract

Massive Multiplayer Online Role-Playing Games (MMORPGs) are a sub-sector of virtual worlds that share with other worlds the characteristics of both complex technological systems and complex societies. The success of several MMORPGs makes them a vibrant area for research from different points of view, including their economic aspects (Castronova, 2005). Our research is mainly concerned with the practice of cheating in MMORPGs and its consequences.

In this paper we explore the economic dimensions of cheating in MMORPGs as they relate to the business activities of companies that offer cheating software, in particular programs called 'bots'. Specifically, we address the following question: "How do cheating practices shape economic interactions around MMORPGs?" We characterize the economy of cheating (as it is carried out by cheating companies) as an answer to breakdowns in the relationship between cheaters and cheating companies (Winograd and Flores, 1987; Akrich, 1992), which involves both learning and innovation processes. In order to answer our question we present a case study of the Tibia (http://www.tibia.com) and an ongoing anti-cheating campaign. In the conclusion of the paper we provide some general reflections on the relevance of the economy of cheating to Virtual Worlds research.

Keywords: economy of cheating; bots; MMORPGs; breakdown; ethnomethodology; ethnography.

"We Will Always Be One Step Ahead of Them"

A Case Study on the Economy of Cheating in MMORPGs

By Stefano De Paoli and Aphra Kerr
Department of Sociology and NIRSA, National University of Ireland Maynooth

Massive Multiplayer Online Role-Playing Games (MMORPGs) are a highly successful sub-sector of the digital games industry[1] whereby players participate in a virtual world (Bell, 2009; Schroeder, 2009) which is persistent, meaning that it runs independently from the user and requires continuous customer support from the game developer (Kerr, 2006). MMORPGs are both highly sophisticated technological systems — in most cases built around a client-server architecture[2] — and 'deeply social' worlds (Castronova, 2005; Taylor, 2006; Acterbosch et al., 2008) in which millions of players chat, co-operate, interact, compete, and trade with each other online through their avatars.

The complex social and technical nature of these virtual worlds make them subject to a range of disruptive practices (ENISA, 2008), including fraud (Bardzell et al., 2007), harassment (Foo and Koivisto, 2004), or social conflicts (Smith, 2004). In our research we are particularly concerned with the consequences of cheating in MMORPGs (see next paragraph for a discussion and definition of cheating), and in virtual environments more generally. Cheating in a MMORPG is a highly contested practice that deserves particular attention, insofar as it is perceived by the developers, publishers, and many players to be a threat to the social experience, economic viability, and security of a game world. For others, cheating is viewed as justifiable because it offers the potential to generate large amounts of real and virtual money, or to more easily make progress in the game rankings.

In this paper we adopt an emergent approach, in particular following some of the methodological principles proposed by Callon (1986), to study how different actors understand cheating within a game and to establish how cheating in MMORPGs shapes economic practices in the real world. In particular we focus on one cheating practice, that of *botting*[3]: the use of computer programs to automate several game tasks (so called bots) in violation of End User License Agreements of games. Specifically, we seek to provide a qualitative account of the socio-technical dynamics (the how) of this phenomenon (Garfinkel, 1967; Latour, 2005). This paper is based on an ongoing case study of the MMORPG *Tibia* (http://www.tibia.com) and focuses on the struggle between its developer and publisher *CipSoft*—which tries to regulate game players—some of whom wish to be able to use bots and some of which do not, and external cheating companies aimed at exploiting player demand for bots. It is a dynamic story that involves learning processes and incremental innovations such as new software tools, including cheating software,s well as new models of governance for the regulation of players' behavior. Our conceptualization of cheating in MMORPGs as an economy is based on ongoing qualitative data analysis of *Tibia* gameplay and Internet forum discussions where we observed that some cheating practices, such as developing, selling, and using bots, are productive and can lead to value creation in the real world.

[1] For statistics on market share, user base and other dimensions of major MMORPGs, see http://www.mmogchart.com

[2] The most common architecture used in MMORPGs is the client-server, which consists of a centralized server (the master) with several clients (the players' machines) connected to it.

[3] See the section *The Case of Tibia and the Cheating Companies* in this paper for a discussion.

This paper consists of a brief critical review of the relevant literature on cheating in online games, followed by a discussion of our research methodology, the findings from our empirical research on cheating, learning and innovation practices surrounding *Tibia*, and finally some general conclusions for understanding cheating and its relationship to the economy of Virtual Worlds.

Cheating in Online Games in a Nutshell

In our investigation of the practice of botting in MMORPGs we follow an approach in which cheating is conceptualized in both technical and social terms (Latour, 1988). In particular we cut across the distinction between social and technical, and we assume reality to be hybrid, composed of a mixture of the two. In this regard our working definition considers cheating as the result or outcome of the relationships between many interleaved social and technical elements (including cheating software, the security design issues, negotiations among players, game companies anti-cheating activities, anti-cheating tools, and in general everything that relates to cheating). We consider our approach, conceptualizing cheating as a socio-technical process, to be useful for the goal of this paper, insofar as it will allow us to investigate the economy of cheating in MMORPGs without operating any a priori reduction to either the technical or the social (Latour, 1988) or making a judgment that cheating is either good or evil (Latour, 1987). However, our approach is substantially different from current literature on cheating in MMORPGs that, in most cases, assumes a strong distinction between social and technical aspects of cheating.

Cheating in games is indeed often just described as a practice which is detrimental to the spirit of fair play and provides unfair advantages to cheaters. A mainstream definition of cheating comes, for example, from Yan and Choi (2002) and states that cheating is "Any behaviour that a player may use to get an unfair advantage, or achieve a target that he is not supposed to" (p. 126). Hoglund and McGraw (2007) even suggest that "Cheats come closest to actual crime when they are used to make a great deal of money." (p. 8). Common examples of cheating in online games include practices such as exploiting bugs and weaknesses in the game design, the use of macros and software to manipulate the game code either directly or indirectly,or even the direct manipulation of other players' trust and social expectations. While the definition of cheating we present here captures some of the elements of this phenomenon; it does not, however, account for all the complexity of cheating in online games. In fact, cheating appears to have a mobile and permeable boundary which is not always easy to define (Consalvo, 2007). Moreover, cheating phenomenology varies according to different games, technologies, motivations, and outcomes (Yan and Randell, 2005).

A further problem in the definition of cheating lies in the differences between the way it is treated in computer science literature as opposed to social or media literature. Most of the technical or computer science-oriented literature on cheating in online games defines it as detrimental to gameplay. The advantages obtained by using cheating techniques are not supposed to be achieved by players (Yan and Choi, 2002). In most cases, it is also said that cheating is due to poor (sometimes non-existent) security design (Yan and Randell, 2005). In this way, such literature reduces cheating to a technological problem: solving the technical limitations of security design will lead to a fair game. Anti-cheating techniques, as formalized in computer

science literature, are supposed to contribute to the achievement of this ideal fair game. Examples of anti-cheating techniques include the use of CAPTCHA[4] 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 cheats in real-time games (Ferretti and Rocetti, 2006).

We are not saying that the computer science or technical approach to cheating in online games is necessarily wrong but we feel that it is limited, to the extent that it is one-dimensional and tries to reduce cheating to a technical or security design problem. In this regard we feel that media scholars and game-studies scholars provide a richer approach by pointing out that cheating is a multidimensional problem, and one which is the subject of conflict among different groups.

For example, Fields and Kafai (2009) describe the case of an educational website where teenagers were able to engage in complex learning activities which included the discovery of smart cheats for solving casual[5] science games. By conceptualizing cheating as a form of learning, Fields and Kafai provide an example of how the reduction of cheating to a technical problem is clearly a limited approach. Another example is Smith (2004), in which cheating in online games is described as 'extra-mechanical conflicts' (together with, for example, norms violations or grief play[6]) that are the direct consequences of the social spaces created by these games. This is as opposed to 'intra-mechanical conflicts' (for example the conflict that arises when one plays against another in a first-person shooter game), which results directly from the game rules (results explicitly from its design) and are therefore not disruptive. The work by Smith shows that cheating relates to the complex social space generated by these games. A further contribution to the debate on cheating is made by Kücklich (2007 and 2009), who has suggested using cheating as a methodology to explore non-obvious aspects of digital gameplay, including its machinic/cybernetic processes: an approach that he defines as *deludology*.

The study by Consalvo (2007) constitutes perhaps the main example of how media studies conceptualize the multidimensionality of cheating. Indeed, for Consalvo (2007) cheating in online games is something that gets culturally negotiated by players, cheaters, and the anti-cheating industry, and she seems to suggest that a single definition does not help in understanding its cultural and dynamic character. In this regard Consalvo notices that often what is at the centre of the players' negotiations are what she calls 'soft rules', or in other words those game rules that do not depend directly on the game code (the so-called 'hard rules') and that "can be broken more easily than the game code" (p. 87). Consalvo's work takes into account not only social and cultural dimensions but also, in part, the technological dimensions. For example, the whole of Chapter 6 provides an analysis of the different cultural attitudes existing in the anti-cheating industry and an analysis of different anti-cheating strategies. Although we recognize some links between our work and that of Consalvo, and its influence on our own conceptualization of cheating, we are of the opinion that more empirical research will need to be done in order to better frame how cheating is practiced in MMORPGs.

In conclusion it is our opinion that media and game-studies literature on cheating goes in the opposite direction to computer science literature. In media research, cheating is described as negotiated and permeable and is also often reduced to social or cultural elements. When reading

[4] Completely Automated Public Turing test to tell Computers and Humans Apart.
[5] A 'casual' game is a video game or online game targeted at a mass audience of casual gamers.
[6] Grief play is when a player intentionally disrupts the gaming experience of other players (Foo and Koivisto, 2004).

media literature it is also not uncommon to recognize the specific implication that cheating can be evidence of player power and resistance. Therefore what we have in the literature on cheating in online games is a continuum that goes from a purely technology-focused world (the lack of security design) to a purely social world, whereas both ends of the continuum grasp some aspects of the phenomenon of cheating.

The Theory and Method of Our Research: An Emergent Approach

Our approach to the study of cheating in MMORPGs emphasizes the accounts that are provided directly by the actors themselves: the various cheating companies, their customers, game developers and publishers, and finally how non-cheating players see and define cheating. Moreover, we include as actors how game design, cheating and anti-cheating software, and licenses enter into the picture as active elements of concrete negotiations. In doing so, we follow an important research tradition that relates to the phenomenology of technology, ethnomethodology and Actor-Network Theory (see in particular Garfinkel, 1967; Callon, 1986; Winograd and Flores, 1987; Akrich, 1992; Latour, 2005).

In particular we adopt the principle whereby the observer does not decide in advance the social and technical attributes of the technological system (or virtual world in our case). Instead, we consider the attributes to be *ethnomethods* (Garfinkel, 1967) that emerge from the negotiations surrounding the virtual world. Ethnomethods are native conceptions, terminologies, explanations, and in general methodologies used by the actors to make sense of the world they inhabit. These native conceptions and methodologies are epistemologically opposed to those of a possible (and fictional) external scientific observer educated in the relevant scientific domain (Lynch, 2007). This also implies that the observer is required to not impose or implement in advance a theory to explain or understand ethnomethods. Michael Callon (1986) describes this emergent approach as follows: "the observer must consider that the repertoire of categories which he uses, the entities which are mobilized, and the relationships between these are all topics for actors' discussions. Instead of imposing a pre-established grid of analysis upon these, the observer follows the actors in order to identify the manner in which these define and associate the different elements by which they build and explain their world, whether it be social or natural." (pp. 200-201).

According to Akrich (1992), one of the key methods for approaching the problem of how the actors build and explain their world is to focus on the moments of rupture that occur in the "natural flow of things," and in particular on those situations in which devices and technologies go wrong. The author observed that we need to focus on disputes around technological or device failures as the crucial moments that reveal the actors' activities and ethnomethods. Winograd and Flores (1987), in their pivotal work on the design of computer artifacts, proposed the specific term *breakdown* in order to capture these moments of rupture. During breakdowns, the objects that populate the world we inhabit (again, often technological systems–think about your car or your laptop) and that we take for granted (and that therefore lie unobserved in the background) become particularly evident or present to us as they become the subjects of controversies, negotiations. and adjustments. Indeed, when technological devices break down, actors become aware of their presence and importance, and most importantly, they undertake a series of actions to fix the broken devices. It is therefore during breakdowns that we, as observers, can be direct witnesses to the actors' efforts to bridge and solve the ruptures. In other words, the concept of

breakdown provides us with a concrete way of approaching the 'how' of the economy of cheating as ethnomethod: something that reveals its fundamental traits and attributes during the disputes and negotiations around the technological aspects of cheating practices.

As described before, a key element of this approach is to focus on the relevant social groups in innovation processes. Users are in many cases one of these groups. 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; Woolgar, 1991; van Oost, et al., 2009). In the innovation process, users can have indirect roles (through, for example, market research) or more direct roles (for example, usability testing and participatory design). Their tacit layman's knowledge can provide important inputs to the innovation process,but can also lead to its failure. Another relevant social group in innovation processes is that of technology designers and technology builders in general, whose task is often to inscribe patterns of use in the technologies they create, hence envisioning a possible evolution of society (often referred to as a 'script', see Akrich, 1992; Latour, 1987) through technological means.

The data in this paper draws upon a virtual ethnography (Hine, 2000) of the game *Tibia*, the official *Tibia* forums, and the forums of cheating companies who develop bots for *Tibia*[7]. This paper draws in particular on the forum threads directly related to an anti-cheating campaign launched in early 2009 and discussed both on official *Tibia* forums (a total of 379 threads) and on cheating companies' forums (a total of 442 threads)[8]. The data gathered from the forums was supplemented by participant observation within *Tibia* and included the creation of a character that was played for at least six hours each week on a PvP server[9] since February 2009. Game play has enabled us to interact with players, understand the gameplay's dynamics, and understand the use of language and terminology in the game[10].

Our mixed method approach allowed us to capture spontaneous discussions and negotiations on the forums[11] and to understand these in relation to gameplay. In terms of data analysis, our approach followed that proposed by Latour (1988, p. 10) which suggests that one follow the 'storytellers' (i.e. the main actors and groups) and how they attribute causes, endow entities with qualities or classify actors, in line with what was previously described. This approach enables us to provide a dense account of how the actors and relevant groups themselves describe the world they inhabit (their ethnomethods), without trying to impose a predetermined grid of analysis. In this paper we present forum messages and other data produced by the *Tibia* storytellers (Cipsoft the *Tibia* developer, the cheating companies, and the players both cheaters and honest ones). These data have been selected as illustrative examples of the wider and

[7] Official *Tibia* forums are at the following URL: http://forum.tibia.com/forum/?subtopic=communityboards. Cheating company forum URLs: http://www.blackdtools.com/forum/ and http://forums.tibiabot.com/

[8] The threads on both the official and cheating companies' forums are of different lengths, ranging from just a few posts and spanning a few days, to threads composed of more than 4000 posts and spanning more than one year. An average thread is composed of 5-6 pages (100-120 posts), and might last a few months.

[9] PvP stand for Player versus Player, a type of gameplay in which players compete directly with one another.

[10] The in-game observations have been useful for acquiring knowledge about how players relate to each other and with Non-Player Characters, including for example the differences between characters' roles, the geography of *Tibia*, and knowledge about the different monsters and quests in Tibia.

[11] The forum threads were collected using the Web-archiving software Scrapbook; see http://amb.vis.ne.jp/mozilla/scrapbook/. Scrapbook provided us with organized storage and easy retrieval of the data. Scrapbook is an extension (add-on) for the web browser Firefox that allows one to save and manage collections of web pages and web sites in a convenient way.

ongoing activities related with the key disruption of the existing stable market relationships between cheating companies and cheaters, occurred at the beginning of the anti-cheating campaign.

The process of research and analysis of the *Tibia* case study is ongoing, and while in this paper we follow closely the approach proposed by Latour we are also, in the current phase, conducting a Grounded Theory (Charmaz, 2006) to the main forum threads and documents (including Tibia legal documents and official articles). With Grounded Theory the theory emerges thorough a recursive and inductive iteration between data and theory. Thus, this paper provides an overview of one part of a much larger project which we hope will contribute a great deal more to the empirical and theoretical understanding of cheating in MMORPGs.

The Case of *Tibia* and the Cheating Companies

Tibia is a 2D medieval 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 total subscriber base of 300,000 players, 100,000 of which have premium accounts (CipSoft, 2008). In *Tibia* there are two types of accounts: free and premium, and one player may have several accounts. The price of a Premium account varies depending on the length of the period paid for. Currently, buying a Premium account for 12 months costs EUR 4.99 per month, whereas only one month costs EUR 7.45. Premium accounts benefit from additional advantages compared to Free accounts, including, for example, premium areas that cannot be accessed with a Free account, a large number of abilities for premium characters, large storage spaces for items, and also the possibility to become the leader of a guild, something that is not allowed for players with Free accounts.

Although *Tibia* does not possess powerful 3D graphics such as those you can find in other MMORPGs, its role-playing elements and the Player Versus Player features are what make it attractive to players. *Tibia* players can choose among four different types of roles (called vocations) that include Knights, Paladins, Sorcerers, and Druids. A character's vocation determines her characteristics in many ways, which it would not be possible to describe here in just a few words. The different vocations allow different types of gameplay, especially concerning attacks and combat with both monsters and other characters. Knights, for instance, are stronger in using 'melee' items (such as swords or axes) and are therefore more powerful in close combat. On the other hand, Druids are stronger in casting spells and healing. In *Tibia*, players can engage in different role-playing activities, including quests that can be solved by a single player, or by forming a team of players composed of characters with different vocations. The killing and looting of *Tibia* monsters is certainly one of the main activities of the game, since this provides 'experience points' that enable a character to make progress in the game rankings.

Figure 1. *Tibia* screenshot that shows a character (Talah Teon) engaging in combat with monsters (Slimes and Bats). We can see the game interface with the character's items on the right, the game map on the upper right and the game chat at the bottom of the screen. (From http://www.tibia.com/abouttibia/?subtopic=screenshots&screenshot=cathedral)

Another relevant feature of the role-playing in *Tibia* is that players can form guilds and take part in wars among these guilds. The rewards for winning a guild war lie in the ability to exercise forms of domination over a server, as powerful guilds are regarded as having "more influence on the events and politics in a world than any single player could possibly have, and few will be foolish enough to mess with a member of a strong guild" (CipSoft, 2009b). Guilds can rent houses in the game cities and create their own headquarters where characters belonging to the same guild can meet; in these houses players can also store items or restore lost points faster, after losing them in fights.

Figure 2. *Tibia* screenshot that shows the medieval fantasy atmosphere of the game. In the picture several characters fight each other in a guild war. (From http://www.tibia.com/abouttibia/?subtopic=screenshots&screenshot=guildwar)

Tibia was chosen for this case study on cheating because CipSoft, the company that develops and distributes the game, started a campaign against cheaters at the beginning of 2009. Since then *Tibia* players have experienced mass bans of cheaters, changes in regulations, and the introduction of new software (including both cheating and anti-cheating tools). In *Tibia*, cheaters, especially so-called 'botters', were considered quite widespread by the player community, which had asked CipSoft several times in the game forums to take action to solve the problem[12]. 'Botting' is the practice by which a player uses an external computer program, known as a *bot*, to automate certain gameplay tasks. These 'bots' operate via "artificial intelligence routines pre-programmed to suit the game map, game rules, game type and other parameters unique to each game" (Computer Game Bot, 2009). As in many other MMORPGs, *Tibia* players must perform certain actions such as killing and looting monsters in order to acquire special items or virtual currency, or to increase their ranking and levels. In most MMORPGs, accumulating items and currencies and leveling up a character[13] can be a long and

[12] See for example this long thread in which players asked for the deletion of cheater accounts: http://forum.tibia.com/forum/?action=thread&threadid=1978162

[13] 'Levelling up' means enabling a character to move to a higher level of competence, which gives him/her more value in the game.

time-consuming process (Kolo and Baur, 2004), which many players find tedious. Killing and looting monsters are indeed often repetitive and boring activities, and bots can assist or even totally replace the players (so called *Away From Keyboard* play, or AFK) in performing these tasks (Golle and Ducheneaut, 2005). As Joshi (2008) mentioned, bots can run forever without getting bored or tired like human players.

CipSoft has never directly asserted the possible relationships between its revenue and the campaign against cheaters/botters. However, on the game forums several players declared their intention to stop paying for their Premium game accounts because of the presence of cheaters. It is also clear that the use of bots has a direct influence on gameplay, the negative impact of which is clearly perceived by fair players in many ways:

> *For too long, the botters have ruined our economy, our society, our enjoyment of this game. We the few, the noble, the honest stand here before CipSoft today and demand a change.*
> (From http://forum.tibia.com/forum/?action=thread&threadid=1978162&pagenumber=99 Post #19615799, July 18, 2008)

Therefore CipSoft's anti-cheating campaign is probably a response to complaints made on the forums[14] by many within the player community about the spread of cheaters, and to player requests for a stronger policy against cheaters. A manifesto article that summarizes the company's anti-cheating strategy states:

> *In short, we do not want cheaters in Tibia. We are of the opinion that they directly destroy the economy and have a negative influence on the peaceful gameplay of fair players.* (CipSoft, 2009a)

On the other side, two cheating companies, *BlackD* and *NGSoft* (which operate within the law in their home countries), 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. Their programs include several different bots (*BlackDProxy*, *elfbot*, *TibiabotNG*), all of which offer different types of cheating features. The price of the bot license varies depending on the number of computers on which the bots are used and the length of the purchase period[15]. What follows is an advertisement for the bot TibiabotNG on the NGSoft website:

> *TibiaBotNG is a professionally crafted client modification for the massive multiplayer online role playing game called Tibia. It is the first product around to offer the benefits of full integration into the Tibia client, making any addition to it both natural and powerful.* (From http://forums.Tibiabot.com/, Retrieved September 28, 2009)

As we can see this software is described as a "professionally crafted" modification of the *Tibia* game client, and is portrayed as "natural and powerful." This bot comes with several features[16] that facilitate gameplay including, for example, assistance during battles, scripting

[14] See again this huge thread, where players asked for the deletion of the account as punishment for cheating http://forum.tibia.com/forum/?action=thread&threadid=1978162

[15] The licence for the bot BlackDProxy, for example, is worth EUR 10 for one computer for a one-year period. See http://www.blackdtools.com/purchasefull.php

[16] For TibiabotNG features, see http://www.tibiabot.com/features.php

facilities, or AFK play that in itself includes features such as auto-healing (restoring points lost in fights) and auto-looting.

To counter them, the ongoing anti-cheating campaign by CipSoft has included the mass banning of game cheaters' accounts (one mass ban per month since the end of January 2009, with approximately 5,000 accounts being affected each time), new anti-cheating tools, and changes to the game's regulatory policies. During this period 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 (EULA) or the Terms of Service. Consalvo (2007, ch. 6) identifies and describes three different types of tools[17]: (1) tools that seek to prevent cheating (for example by the mean of encrypted communication between server and clients), (2) tools that seek to render cheating ineffective (for example by disconnecting the cheater once detected) and finally (3) tools that seek to detect the use of third party software (such as bots) that tamper with software clients[18] and that, as an outcome, allows game companies to ban the cheaters on the basis of the detection. The anti-cheating tool introduced in *Tibia* is of this third type and aims to detect unofficial software used to play the game. One of the mass bans (April 2, 2009) carried out by CipSoft was announced on the 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.*
> (From http://www.tibia.com/news/?subtopic=newsarchive&id=962&fbegind=4&fbeginm=3&fbeginy=2009&fendd=3&fendm=4&fendy=2009&flist=11111111)

In this message CipSoft clearly emphasizes that the banning action was undertaken on the basis of information on the use of unofficial software gathered by the anti-cheating tool. This same emphasis is also placed on the banning messages sent to cheaters and displayed on players' accounts, as the following figure shows.

Figure 3. Example of a banishment notification on a cheater's account, showing the automatic detection of unofficial software.

The new automatic anti-cheating tool clearly interferes with both the practices of cheaters and the business of the external cheating companies. Indeed, the campaign against cheating and the introduction of the anti-cheating tool are elements that change the current configuration of the situation: it is a real moment of breakdown for cheating companies. Before this anti-cheating campaign, it was common knowledge that using bots in *Tibia* was easy. On the official game forums several players, in different threads, described the plague of the diffusion of botters on

[17] Known examples of anti-cheating tools for Online Games are Punkbuster or GameGuard. For a discussion, see Consalvo (2007), Chapter 6.
[18] The use of a Tibia bot is a modification of the game client that is forbidden by the game's legal documents.

game servers and in hunting areas[19]. Meanwhile, on the cheating forums cheaters shared images--or even videos--of what they called *projects*: the creation of powerful main characters (the projects) leveled up by using bots[20]. The introduction of the anti-cheating tool has, however, radically modified the situation for cheating companies and cheaters and has broken the existing stable market relationships between these groups. It is especially clear that these relationships were strongly based on the ability of bot programs to remain undetected. This breakdown has also lead cheating companies to declare their ambition to develop a new detection-safe version of their bots as a way to re-stabilize market relations with their customers. Thus, the development and deployment of an anti-cheating tool--and the resulting breakdown--have triggered a new process of learning and innovation for both cheating companies and cheaters.

Cheating as a Supply and Demand Relationship

CipSoft introduced the first mass ban at the end of January 2009, one month after the publication on their website of the manifesto article describing their new anti-cheating strategy. This mass ban was unexpected by all concerned: honest players, cheating players, and cheating companies. Many honest players described the bans and the introduction of the anti-cheating tool as a good starting point in the campaign against cheaters. By contrast, for the cheating companies the mass ban constituted a serious threat to their cheating business, while cheaters have often described the new situation as the end of botting. After the mass ban many bot customers were particularly worried about the new situation. What follows is an example, among many, taken from a cheating forum:

> *I did not get banned i'm merely pissed off at LoW claiming its safe, its a fucking hoax that works only because you're a bunch of brainless monkeys.*
> (From http://forums.tibiabot.com/showthread.php?t=111778 Post #9, February 9, 2009).[21]

In this message a customer complains to LoW (Lord of War, who we take to be one of the owners of the cheating company NGSoft) about his claims that the use of bots is safe, despite the mass bans and the introduction of the anti-cheating tool. After the mass bans many bot customers became afraid to use these programs when playing *Tibia*, as the following example demonstrates:

> *I'm kinda afraid of loggin it on this computer with bot installed...*
> (From http://www.blackdtools.com/forum/showthread.php?t=35826 Post #1, March 1, 2009)[22]

Although many other cheaters declared their will to continue to use bots despite the mass bans, it is also clear from the above message that cheaters were facing a challenging situation. In

[19] See for example this discussion: http://forum.tibia.com/forum/?action=thread&threadid=1978162
[20] See for example this discussion: http://www.blackdtools.com/forum/forumdisplay.php?f=47.
[21] This message comes from a thread that has been removed from the forum by the cheating company. Indeed, several threads have been removed by the administrators of the forum and appear to be accessible only with administrative rights. All the data presented here and not available online can be received by specific request to the authors of this paper.
[22] This thread has been officially removed from the forum by the cheating company. What is reported here is the original URL. See footnote 21 for an explanation.

particular they had to decide whether to continue botting or not. What follows is a poll that was launched on one of the cheating forums after the first mass ban, which asked "Are you botting?"

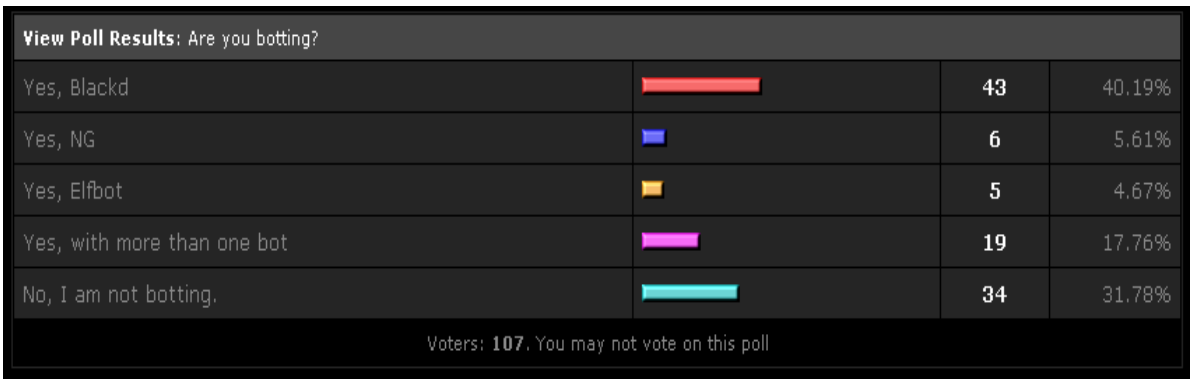

Figure 4. Poll – on BlackD forum – about the use of bots (From http://www.blackdtools.com/forum/showthread.php?t=36002, February, 02 2009)[23]

Although this poll does not have statistical validity, it shows (in the last line) that almost one third of respondents (34/107) declared that, at the time of the poll, they were not using bots as consequence of the first mass ban. The introduction of the anti-cheating tool has changed the relationship between cheating companies 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 many players are still botting but just over a third are not, and if CipSoft further increases the risks for players this could lead to a decrease in the demand for bots and consequently a decrease in revenues for cheating companies. However, this new configuration of things is also what triggers new dynamics in cheating companies' business practices, since they need to respond to changes in customer demand:

> *i have the utmost faith in blackd and i am certain that he will get a completely undetectable bot in the near future...but, you all must give him some time.*
> (From http://www.blackdtools.com/forum/showthread.php?t=39151 Post #1, April2, 2009)

Indeed, bot users now have the expectation that companies will create a new generation of undetectable bots. The actions undertaken by cheating companies in order to cope with the breakdown--and with the new customer demand--are described in the following paragraphs.

[23] This thread has been removed from the forum too. See footnote 23 for an explanation.

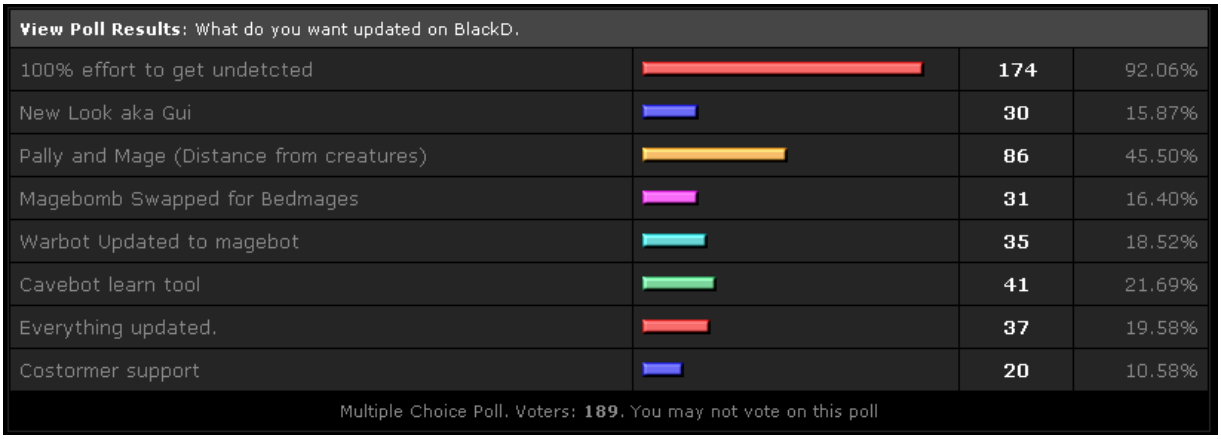

Figure 5. A change in market demand: A poll from a BlackD forum that shows the demand from cheaters for bots with 'undetectability' capabilities. The poll has no statistical validity but shows the high request rate (174/189 respondents) for undetectability of bots (From http://www.blackdtools.com/forum/showthread.php?t=41398 June 3, 2009)

Cheating as a Learning Process – Player/Firm Interactions

One of the key issues of this story is that the cheating companies do not know how the CipSoft anti-cheating tool operates, and this creates a problem for the development of new undetectable bots. This is not just an accident; it appears to be 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, February 2, 2009)

So, as a general strategy against cheating companies, CipSoft does not want to reveal anything about the anti-cheating tool. For cheating companies, however, in order to meet the new customer demand for undetectable bots it becomes essential to acquire some knowledge of how the anti-cheating tool works. Fields and Kafai (2009) 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*, the cheating companies and players who are their customers are involved in a collaborative 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 their learning process is to develop a way to defeat a cheating counter-measure: the CipSoft anti-cheating tool. On the *Tibia* cheating forums this learning process is pursued by making deductions based on the behavior of the game client (after the tool's introduction), or 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 [sic] that always at start then it would bee [sic] too easy to catch that packet.*
> *I will appreciate help from people who can read hex, and know about the API*[24] *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, Post #1, January 30, 2009)

It is interesting to see how cheating is a socio-technical process that involves a learning process, in which various technological elements (for example installed programs, APIs, calls to functions) form cheating business practices. In this case BlackD guesses that the anti-cheating tool operates by searching for well-known strings (such as bot programs' installation names) on users' computers. If these strings are found, then the tool will report this information to CipSoft. 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 to confirm/refute this theory. What follows is an example of this learning process, with a cheater providing some feedback 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=5 , Post #45, January 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 workings of the anti-cheating tool, again proposed by BlackD:

> *THEORY 2:*
> *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, Post #1, January, 30 2009)

In this case the company proposes the idea that the anti-cheating tool scans the players' chat logs searching for known strings (for example "blackd" or " tibiabot") related to bots. The idea is that if a player has written certain strings several times in the chat while communicating with others players (see Figure 6 for an example that clarifies this point), in a given period of time, then this is detected by the anti-cheating tool. The decision to ban cheaters will be based on

[24] Application Programming Interface - the details of how a programming language is to be used. Programmers wishing to change or add to existing code need to know these details.

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, Post #45, January, 30 2009)

In this case we have a positive deduction based on the consideration that the cheater has used the strings numerous times in chats but he/she has not been 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, Post #61, January, 30 2009)

The second theory is therefore contradicted by the consideration that cheaters got banned even if they had never used those strings in the chat while playing the game.

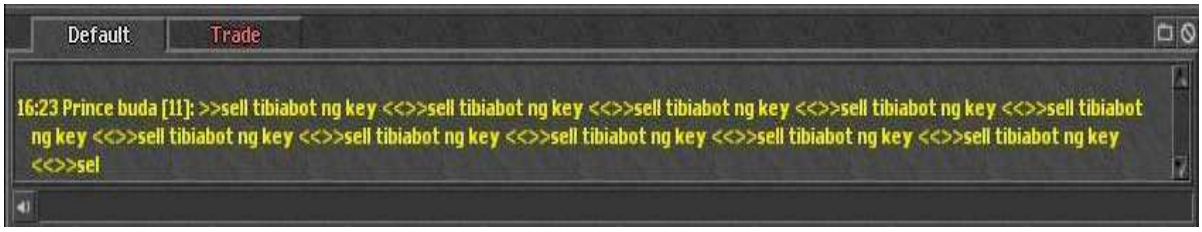

Figure 6. Example of a chat log with the name of a bot (TibiabotNG) repeated several time. From http://www.tibiapic.com/show.php?v=fPSwcgTzTTTT

The evidence gathered and presented above 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 and how it detects the cheating software: the process is as social as it is technological. It is also crucial to see how this learning process involves close interactions between cheating companies and the cheaters that are invited to contribute to the learning process. In other words, cheating companies try to mobilize external human resources for their technical knowledge of the game client and the gameplay, in their goal of creating a new generation of bots.

Cheating as Part of an Innovation Process

Cheating in *Tibia* results in multiple and ongoing innovations by a range of different actors. CipSoft's anti-cheating campaign since January 2009 has involved the introduction of two innovations: the anti-cheating tool and new governance policies. These have forced the cheating companies to start a process of research and development which is resulting in

incremental product innovations (a new generation of bots) to combat the anti-cheating tool. For the cheating firms, this process involves them gathering feedback from players about their use of cheating 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 thus maintain their business.

For cheating companies the innovation process is attempting to do two things: develop undetectable bots and reassure customers so as to stabilize relationships with them. The following message by NGSoft clearly aims to reassure those customers who have become afraid to use bots because of the mass bans, and predicts 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, February 01, 2009)

As we can see, the company (NGSoft in this case) clearly declares the will to initiate an innovation process based on research and development activities. Moreover, the customers are reassured that this new generation of bots will be safe to use. A similar attitude is maintained by the other cheating companies, as the following message taken from the BlackD website shows:

> *No matter how many changes CipSoft do, we don't surrender. We keep updating our bot and we keep improving the stealth*[25] *functions. We will always be 1 step ahead of them.*
> (From http://www.blackdtools.com/news.php?p=2 March 23, 2009)

In BlackD the innovation process toward a safe, undetectable bot has taken on the specific name of 'stealth'[26]. This definition of innovation recalls military efforts to make war technologies less visible, if not undetectable, by enemies. Moreover, as part of an overall strategy, BlackD has decided not to release to the public any information on the bot that might help CipSoft create counter-measures:

> *We have decided that we will not release the code of Blackd Proxy core anymore: we won't release an updated Free Proxy. That way CipSoft won't be able to spy our new technology. [sic]*
> (From http://www.blackdtools.com/news.php?p=2 March 23, 2009)

In fact new versions of bots were released shortly after the first mass ban (January 30, 2009), incorporating several enhancements that were supposed to counteract the anti-cheating tool. These enhancements included for example several forms of randomization of gameplay actions in order to make the bot acting more like a human player, or the removal of bots installation names from the client machines[27]. These incremental innovations were also based on

[25] 'Stealth' specifically refers to the property of undetectability in bots.
[26] See, for example, this thread, post #358 for further details:
http://www.blackdtools.com/forum/showthread.php?t=35800&page=36
[27] Some of the stealth capabilities of BkackDProxy are listed here:

the information provided by cheaters via public forums. Interestingly, the first mass ban has been followed by others (one each month since January 2009, with approximately 5,000 accounts banned each month[28] and more than 45000 accounts banished in total so far). These subsequent bans constitute a dynamic situation in which the new bots were being tested in the marketplace. For example on BlackD forums, cheaters were asked by the company to provide feedback on characters created after the first mass bans and played with the new stealth bots:

> *In order to get proof of the new safety...Please bot a new character only using new updated version.*
> *We will see the results in the next mass ban day.*
> *Note that your old characters might have been already marked to deletion in that next day, even if you don't login them again from now. [sic]*
> (From http://www.blackdtools.com/forum/showthread.php?t=36243 Post #1, February 6, 2009)[29]

As we can see, the company makes an explicit request to its customers: to create new characters and to play them with the new version of the bot. This explicit request is made because deletion information might have already been gathered for characters that were played with bots before the (first) mass ban and before the introduction of the anti-cheating tool. On March 03, 2009, CipSoft carried out a second mass ban. While many cheaters reported that their newly created characters were not banned in this second wave, some did report banishments, as the following case clearly exemplifies:

> *YES I GOT BANNED WITH ONE. Created AFTER the proxy improvements*
> (From http://www.blackdtools.com/forum/showthread.php?t=37571, Post #6, March 3, 2009)[30]

The new enhancements to the BlackD bot, introduced after the first mass ban, were therefore not effective. In March, after the second ban, the company BlackD was still declaring on its website that the use of bots was safe and that they were still working on a stealth approach. 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.*
> *Anyways you can still get profit from farmers and transfer that gold to your main character later.*
> (From http://www.blackdtools.com/news.php?p=2 April 2, 2009)

---

http://www.blackdtools.com/forum/showthread.php?t=11&highlight=stealth&page=7, message #63.

[28] For some players the impact of each mass ban is relatively low, accounting for only 2-3 botters banned each day in each server (5000 accounts / 74 servers, with therefore an average of 68 accounts banned on each server in a month), see http://forum.tibia.com/forum/?action=thread&threadid=2712834

[29] This thread has been removed from the forum too, see footnote 21. What is reported here is the original URL with the date of publication.

[30] This thread has been removed from the forum. The URL provided is the original. See footnote 21.

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 given specific advice on how to use bots. In particular, the company BlackD has invited cheaters not to use bots for their main characters. Instead, BlackD has suggested that the bots might be used for secondary characters (gold farmers) that can subsequently transfer their loot to the main character. It is clear that having a main character banned from the game because of cheating is a major loss for cheaters, whereas risking a ban on a secondary character--created with an account different from that of the main character--is sometimes an acceptable risk.

In any case it is clear that so far no secure and undetectable bot (a stealth bot) has been created and that 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 cheaters are being banned on a regular basis by CipSoft and the tool. Therefore, while cheating companies have been innovating as an answer to a mutation in market demand from their customers, they may not succeed in the marketplace.

The Economy of Cheating in MMORPGs: Reflections for Virtual Worlds Research

In this paper we have explored how one form of in-game cheating (botting) can lead to innovations in the real-world economy, and how these innovation processes are triggered by a mutation of conditions in a marketplace. We think that this paper provides a useful contribution to our understanding of the relationship between virtual worlds and the real economy, insofar as it has unveiled and described an 'underground' economy and its socio-technical practices. In particular the adoption of an emergent approach based on ethnomethodology (Garfinkel, 1967; Callon, 1986; Latour, 2005) has proved to be a promising avenue for this type of qualitative investigation into virtual worlds. While we are unable to quantitatively assess the extent of cheating in the game, this approach allows for an in-depth assessment of particular socio-technical practices over time and accords equal status to the different perspectives of a range of actors.

In the case of *Tibia* what we have is a clash between the business of a MMORPG company and the business of cheating companies. Indeed, this case study reveals that cheating companies do their business 'just' within the boundaries of the *Tibia* game. The business of developing and marketing bot programs that tamper with game clients exists because the MMORPGs exist. In particular this study has shown that cheating innovation is a dynamic and productive process which is based on research and knowledge-acquisition activities as well as on incremental results based on market testing. Cheating innovations in *Tibia* are a collaborative process of learning and knowledge-development which increasingly takes place in socio-technical networks, rather than purely internally in companies, and involves a range of social and technical factors. Therefore, in this study we have tried to unveil both how cheating can be productive in a very real sense and also to show the underlying socio-technical complexity of the relationship between cheating companies, their customers, and *Tibia*.

In this case study we have described how cheating companies have faced a breakdown in their business and how these companies have tried to cope with this breakdown and with the subsequent user demand for undetectable bots. As Callon (1999) pointed out in his contribution to the study of the market as a socio-technical phenomenon, responding to this kind of rupture

requires a new configuration, a new framing, of the existing network of socio-technical relations: this is necessary because a certain amount of work has to be done and investment made in order to make relations calculable again. And indeed the breakdown introduced by the anti-cheating tool has required cheating companies to work towards the reshaping of a new set of relationships among themselves, their customers, and their products in order to re-frame a certain order and stability. The concrete answer to the breakdown is the creation of a new generation of bots with stealth capabilities, totally secure from detection by the anti-cheating tool. The goal of this technology (the stealth bot) is to recreate a new set of stable market relationships between the cheating companies and the bot customers. So far, however, this innovation and the new generation of bots have not been successful and CipSoft's anti-cheating campaign seems to be effective in counteracting certain types of automatic cheating in *Tibia*.

At a more general level, while cheating conveys an unfair advantage to some players in virtual worlds, it can also be said to generate productive activities and value in the real economy. In the case examined in this paper cheating generated the production and ongoing innovation of anti-cheating and botting tools. Castronova (2005), in his inquiry into the social and economical dynamics of synthetic worlds, has pointed out that MMORPGs have important implications for labor markets and for the creation of revenues. Complex economies are behind--and embedded in--these games, and they create jobs and wealth in ways that were perhaps unexpected and largely not understood. In our opinion cheating companies that focus on MMORPGs constitute an unexplored dimension of how MMORPGs can generate revenues and labor markets. By saying this, we do not mean to justify the existence of any cheating business that creates jobs and revenues. However, it is important to recognize that cheating companies such as those described in this paper operate exactly as 'normal' software companies do. These companies sell cheating software on the real-world market in exactly the same way as any other software companies: users need to pay a license fee for limited use and on a limited number of machines. In our opinion, the activities of producing, selling, and using cheating software to tamper with game clients or to intercept server-client communications--in contravention of the games' EULAs--are not justifiable per se. However this position cannot deny the empirical evidence that there is a complex economic dynamic in place. In particular, as we have seen, we have companies that have a business, we have customers that demand innovative products, and in general we have networked market dynamics that emerge at the boundaries of MMORPGs. Therefore some forms of cheating practices, such as developing, selling, and using bots are productive processes that lead to value creation in the real world. We are convinced that a better understanding of the productive nature of cheating may lead to more acceptable solutions to the problem of cheating in MMOPRGs for all the actors involved.

Acknowledgements

The authors would like to acknowledge the support of the Irish government’s Higher Education Authority under the PRTLI 4 programme and their partners on the 'Serving Society: Future Communications Networks and Services' project (2008-2010).

We also thank the two anonymous reviewers for their insightful comments.

Bibliography

Achterbosch, L., Pierce, R., & Simmons, G. (2007). Massively multiplayer online role-playing games: the past, present, and future. *Comput. Entertain.*, *5*(4), 1-33.

Akrich, M. (1992). The de-scription of technical objects. In W. Bijker& J. Law (Eds.), *Shaping technology/ building society* (pp. 205-224). Cambridge, Mass: MIT Press.

Bardzell, J., Jakobsson M., Bardzell S., Pace T., Odom W., & Houssian A. (2007). Virtual worlds and fraud: Approaching cybersecurity in massively multiplayer names. In *Situated play, proceedings of the DiGRA 2007*, Retrieved May5, 2009, from http://www.digra.org/dl/db/07311.42219.pdf

Bell, M.F. (2008). Toward a definition of "virtual worlds". Journal of Virtual Worlds Research, 1(1), Retrieved September 16, 2009 from http://journals.tdl.org/jvwr/article/download/283/237

Callon, M. (1986). Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St Brieuc Bay. In J. Law (Ed.) *Power, action and belief: A new sociology of knowledge* (pp. 196-233). London: Routledge & Kegan Paul.

Callon, M. (1999). Actor-network yheory: The market test. In Law J. & Hassard J. (Eds), *Actor network theory and after* (pp. 181-195). Oxford: Blackwell.

Castronova, E. (2005). *Synthetic worlds: The business and pleasure of gaming*. Chicago: Chicago University Press.

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. London: Sage.

CipSoft (2008). *Massive multiplayer online gameserver*. Presentation at QuoVadis Conference, Berlin, May 07, 2008. Retrieved September 07, 2009, from http://www.cipsoft.com/files/QuoVadis-MMOGServer.ppt

CipSoft (2009a). *Where will cheaters go from here?*. Online article, Retrieved September 7, 2009, from http://www.tibia.com/news/?subtopic=latestnews&id=910

CipSoft (2009b). *Tibia manual*. Retrieved September 28, 2009, from http://www.tibia.com/gameguides/?subtopic=manual

Computer game bot. (2009, August 29). In *Wikipedia, the free encyclopedia*. Retrieved 21:52, August 29, 2009, from http://en.wikipedia.org/w/index.php?title=Computer_game_bot&oldid=310783612

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* (pp. 139-143). ACM, New York, NY.

Edquist, C. (Ed.). (1997). *Systems of innovations: Technologies, institutions and organizations*. London: Pinter.

ENISA, (2008). Virtual worlds, real money security and privacy in massively-multiplayer online games and social and corporate virtual worlds. Retrieved November 18, 2009, from http://www.enisa.europa.eu/pages/02_01_press_2008_11_20_online_gaming.html

Foo, C. Y., & Koivisto, E. M. (2004). Defining grief play in MMORPGs: Player and developer perceptions. In *Proceedings of the 2004 ACM SIGCHI international Conference on Advances in Computer Entertainment Technology* (pp. 245-250). Singapore, June 3 - 5, 2005. ACE '04, vol. 74. ACM, New York, NY.

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.

Fields, D.A., & Kafai, Y.B. (2009). Cheating in virtual worlds: transgressive designs for learning. *On the Horizon*, 17(1), 1-20.

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). Retrieved September 7, 2009, from http://doi.acm.org/10.1145/1077246.1077255

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

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

Hoglund, G., & McGraw, G. (2008). Exploiting online games: Cheating massively distributed systems. First: Addison-Wesley Professional.

Joshi, R. (2008). Cheating and virtual crimes in massively multiplayer online games. Technical Report RHUL-MA-2008-06, January 15, 2008 (Department of Mathematics, Royal Holloway, University of London, 2008). Retrieved September 19, 2009 from http://www.ma.rhul.ac.uk/static/techrep/2008/RHUL-MA-2008-06.pdf

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

Kolo, C., & Baur, T. (2004). Living a virtual life: Social dynamics of online gaming. *Game Studies*, 4(1) (Nov. 2004). Retrieved September 28, 2009 from http://gamestudies.org/0401/kolo/

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

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

Latour, B. (1987a). *Science in action: How to follow engineers and scientists through society.* Cambridge Mass.: Harvard University Press.

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

Latour, B. (2005). *Reassembling the social: An introduction to actor-network theory*. Oxford: Oxford University Press.

Lynch, M. (2007). The origins of ethnomethodology. In S.P. Turner & M.W. Risjord (Eds.) *Philosophy of anthropology and sociology* (pp. 485- 516). Amsterdam: Elsevier.

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.

Schroeder R. (2008). Defining virtual worlds and virtual environments. *Journal of Virtual Worlds Research*, 1(1). Retrieved September 16, 2009 from http://journals.tdl.org/jvwr/article/download/294/248

Smith, J. H.. (2004). *Playing dirty - Understanding conflicts in multiplayer games.* Proceedings from 5th Annual Conference of The Association of Internet Researchers. 19-22 September, 2004, The University of Sussex. Retrieved September 18, 2009 from http://jonassmith.dk/weblog/uploads/playing_dirty.pdf

Taylor, T. L. (2006). *Play between worlds: Exploring online game culture.* Cambridge, Mass.: The MIT Press.

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

Winograd, T., & Flores, F. (1986). *Understanding computer and cognition: A new foundation for design*. Norwood, NJ: Ablex.

Woolgar, S. (1991). Configuring the user: The case of usability trials. In Law J. (Ed.) *A sociology of monsters: Essays on power, technology and domination*, (pp. 58-97), Routledge: London.

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

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. (NetGames'05)*, (pp. 1-9). ACMPress, Hawthorne, NY, USA, October 2005.