The Cheating Assemblage in MMORPGs:

Toward a sociotechnical description of cheating

Stefano De Paoli
National University of Ireland Maynooth
Department of Sociology and NIRSA
John Hume Building, Maynooth Rep. of Ireland
Stefano.Depaoli@nuim.ie

Aphra Kerr
National University of Ireland Maynooth
Department of Sociology and NIRSA
Auxilia Building, Maynooth Rep. of Ireland
Aphra.Kerr@nuim.ie

ABSTRACT

This paper theoretically and empirically explores cheating in MMORPGs. This paper conceptualises cheating in MMORPGs as a sociotechnical practice which draws upon a non-linear assemblage of human actors and non-human artefacts, in which the practice of cheating is the result or the outcome of an assemblage. We draw upon the assemblage conceptualizations proposed in [16] and [8] and on empirical data taken from a pilot study we have conducted during the period September-November 2008 and from an ethnography we are conducting in the MMORPG Tibia (http://www.tibia.com) since January 2009. This game in particular was chosen because CipSoft, the company that develops the game, launched an anti-cheating campaign at the beginning of 2009.

Keywords

Cheating, MMORPGs, assemblage theory, sociotechnical assemblage.

INTRODUCTION

In this paper we conceptualize cheating in Massive Multiplayer Online Role Play Games (MMORPGs) as a sociotechnical assemblage. While much of the literature sees cheating as a set of player (or players) actions that modify the game to obtain unfair advantage over other players, we propose that to understand cheating in MMORPGs it should be conceptualised as the result of an assemblage of heterogeneous (human and non-human) elements. Our aim is twofold. Firstly, we would like to illustrate the sociotechnical nature of cheating in MMORPGs showing how cheating is composed both of highly sophisticated technological elements and complex social elements. In this sense the concept/theory of assemblage as proposed in DeLanda [16] constitutes a useful framework that will allow us to cut across the traditional distinction between technology and society. Secondly, we aim to position our work within the studies on cheating in online games proposing a non-essentialist and empirical approach, that differs from existing

conceptualizations. We think that the theory of assemblage will fulfil both goals, and provide a concrete theoretical basis for future empirical research.

In this paper we provide a description of the cheating assemblage, based on empirical evidence taken from a pilot study we conducted during the period September-November 2008 and from the data collected during a virtual ethnography [29] we are conducting in the MMORPG Tibia (http://www.tibia.com)[1] since January 2009. [2] This game in particular was chosen because CipSoft, the company that develops the game, launched an anti-cheating campaign at the beginning of 2009 [12].

MMORPGs are a sub-segment of the digital games industry in which the games are persistent and thousands of players interact simultaneously in virtual worlds which are hosted and supported by commercial companies in return for subscription or micro-payments. MMORPGs are complex social and technological systems and while we do not provide an in-depth description of MMORPGs here (see [1] and [10]) we want to emphasize the complex and heterogeneous nature of these games in which social and technical elements are inextricably mixed: indeed we think that MMORPGs are a phenomenon that empirically breaks the essentialist division between nature and culture.

There are two main bodies of literature on cheating in digital games (for a systematic classification of cheating in digital games see [51]): the technical and the media literature. Whereas the first emphasizes almost exclusively technical solutions to the problem, the second sees cheating as a complex social problem. We believe that the technical

---

Breaking New Ground: Innovation in Games, Play, Practice and Theory. Proceedings of DiGRA 2009

and the social domains should be considered together. Based on our observations from the pilot conducted at the and of 2008 and from the case study of Tibia, we believe that cheating in MMORPGs is not just the actions of players who wish to obtain unfair advantages but rather the confluence of several heterogeneous elements, ranging from player actions, to official documents, to all the cheating solutions or the anti-cheating techniques that are offered over the Internet. We consider most conceptualizations of cheating in MMORPGs to be inadequate to describe the sociotechnical complexity we have observed and in this paper we propose a *Science and Technology Studies* (STS) conceptualization based on the concept of assemblage [8] and [16].

In this paper we provide a brief literature review of cheating and we describe our approach to cheating as assemblage. This is followed by a discussion of the main elements of the assemblage based on our empirical research. We conclude with some closing remarks on the usefulness of our approach.

CHEATING IN DIGITAL GAMES

Literature in computer science and engineering on cheating in online games is mainly concerned with the description and formalization of anti-cheating techniques. In this literature the main definition of cheating reflects the one proposed by Huizinga [31] that described it as something "*harmful for game play*" (p. 52). Here there is a dialectic between the wide diffusion of cheating (the thesis) in online games and the consequent need for powerful anti-cheating techniques (the antithesis). In this dialectic the desired final synthesis will be that of reaching an idealistic and final stage in which the game becomes fair (free of cheats) for everyone. The literature on anti-cheating techniques for example includes the use of antifraud systems [3] the use of captcha[3] (reverese Turing test) to detect bot users [27], generic anti-cheating protocols [11], techniques for preventing software client modifications [44] and algorithms used for detecting cheating [15] and [22].

Media literature, by contrast assumes that cheating possesses a phenomenological richness that deserves to be investigated as such. However, despite the genuine desire for a more complex definition, cheating is often considered as intentional player actions that relate often exclusively to the gameplay. In other words, what media scholars often seem to forget is the technical element that, by contrast, is central in the technical literature. For example [23] described cheating in online games as a social learning process. Another example is [25] who described cheating as a "*non-diegetic operator act*": an action which is external to gameplay but which modifies the intended gameplay experience. Therefore cheating appears to be a sort of interference with the normal gameflow. This definition of cheating is similar to the conceptualization proposed by [33] that sees cheating actions as a useful methodological tool that can be used to explore the game and push the boundaries of our understanding of the digital game. In a more recent work [34] proposes a "techno-semiotic" approach to cheating that theorizes a distinction/continuum between ruled and unruled spaces in games.

In the landscape of media research on cheating the most complete and probably influential work is the book by Consalvo [14], in which the author conceptualized cheating as a central point of departure for looking at how players understand and enact gameplay practices. Consalvo describes several aspects of cheating in digital games ranging from what she calls the paratexts[4], to market aspects, to technology and the culture of gaming. For Consalvo cheating is something that gets culturally negotiated by players, cheaters and the anti-cheating industry and she seems to suggest that a singular definition does not help in understanding the cultural and negotiated character of cheating. In this paper we adopt a similar approach to Consalvo in terms of defining cheating as culturally and contextually negotiated and in attempting to identify the different elements involved in cheating. However Consalvo appears to assume that cheating is an activity carried out by players, and it is in this respect that we attempt to broaden out the range of elements involved in cheating by conceptualising it as the result of an assemblage of heterogeneous elements.

THE ASSEMBLAGE THEORY

To play a MMORPG one has to acquire or download the software client and install it on a computer. During the installation process a player has to accept several legal documents such as the End User License Agreement (EULA) or the Terms of Service (ToS). The acceptance of these documents by the player enacts a legal relationship between them and the publishing company, where the licenses establish, at least in principle, what they can and cannot do with the game software, either on their own machine or on the game server. To play one has to connect the client to the game server and only at this point can one play the game and interact with other players. In most cases, as [14] states, the player will also navigate the Internet searching for guides, walkthroughs or for playing hints on Internet forums. Here we already see an initial set of relations between heterogeneous parts – ranging from the player, to the software, to the licenses - that constitutes what we can call an assemblage.

Cheating in MMORPGs changes the way some of the elements of the assemblage relate to each other and in addition new elements enter into relations with the others. In fact what we have is a new configuration of the MMORPG's assemblage: this is the cheating assemblage.

---

[3] A captcha is a response test to make sure that a response in not automatically generated by a computer.

[4] For [14] paratexts are the surrounding materials that frame the consumption of digital games.

Cheaters, for example will exploit some of the game weaknesses, or build their own cheating code and macros, or acquire cheating software from the Internet, or will exploit known bugs or even other players. By contrast, the company that produces the game will try to avoid cheating and protect itself and the game using for example anti-cheating tools and legal documents. As we can see several different elements/parts enter into mutual relationship in order to form an assemblage, and cheating we argue should be seen as the outcome of the relations between the elements.

Our approach to the study of cheating in MMORPGs owes much to the "assemblage theory" proposed by DeLanda [16], as well as to the concept of sociotechnical *agencement* (or assemblage) proposed by Callon [8], [9] in his research on economic markets as socio-technical networks. [5] We define an *assemblage* [6] as an open-ended gathering of several different, and sometimes in contrast, elements that can range from material artefacts, to texts, to people or organizations, and that can also include for example cities or biological or linguistic elements.[7] The relations between the elements of the assemblage are non-linear, complex and never predictable, but nonetheless these heterogeneous elements can find an alliance [36], a "sympathy" in Deleuze and Guattari [17] terms, that makes them gather together.

Thinking in terms of assemblage is first and foremost a way of thinking about the relations between the whole and the various parts: for us the relations between the parts that result in cheating in MMORPG. DeLanda [16] clarifies that these relations are not logically necessary as it is for systemic or organic approaches. Indeed in these approaches, that can be found in both natural and social sciences, the concept of system is based on interacting parts that form a whole, in which the relations among parts are necessary and that the failure of one relation leads to the failure of the whole system. For example, the organs that compose a human body are elements of a system (the body) that are in necessary relations with one another (if one organ fails or is missing the whole system fails). In social sciences the concept of "social system" draws on a parallelism with natural systems, in which various institutions (e.g. religion or economy) are necessary for the order and integration of societies (e.g. the absence of religious values might lead to anomy). In assemblage theory the relations among parts are conceptualized differently. Indeed in an assemblage parts (e.g. organs or institutions) enter into the whole as contingently obligatory elements. In other words, the relations can change and the parts can withdraw from one assemblage and enter into other assemblages even with different roles. For example, the office in which we work is composed of elements like computers, desks, our colleagues or the books and the shelves in which the books are stored. Each of these elements is fundamental for the office assemblage but their role is contingent (e.g. the same computer can be used in another office by different people or at home, or another computer can be bought in place of the old one; our colleague can change work and be replaced by someone else or we can be asked to move into another office). This means that the relationships need to be approached from an historical and empirical point of view rather than from a theoretical point as in system theory. The assemblage is therefore emergent (it is not an essence), meaning that it is the result of historical and empirical relations among the parts (e.g. our office configurations can change over time).

We think that two aspects of what [9] described as "*the market as socio-technical agencement*" are particularly useful in approaching cheating in MMORPGs. Firstly, the assemblage is composed of heterogeneous elements and the focus of analysis should be on the relations between the parts and secondly, the assemblage delimits and constructs a space of confrontation and power contestations. [8] In DeLanda's theory the heterogeneous elements of the assemblage are augmented by a double axis (see Figure 1).
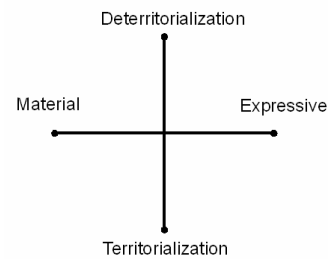

Figure 1: Assemblage: two axis and four arguments

The first axis refers to the material/expressive capacities of the parts/elements of the assemblage. DeLanda [16] follows Deleuze and Guattari [17] in arguing that the material/expressive axis is similar to the difference between a set of laws for regulating an order (discipline) and materially exercising such an order (punish) (see also [45]).

---

[5] Callon, in particular, prefers the word agencement to that of assemblage (see [8] for an explanation), but de facto he also directly refers to the same grassroots of DeLanda, the work by Deleuze and Guattari [17].

[6] Deleuze defines as assemblage as "a multiplicity which is made up of many heterogeneous terms and which establishes liaisons, relations between them, across ages, sexes and reigns – different natures. Thus, the assemblage's only unity is that of co-functioning: it is a symbiosis, a 'sympathy'. (quoted in [16]).

[7] [9] define the socio-technical agencement of the market as composed of "rules and conventions; technical devices; metrological systems; logistical infrastructures; texts, discourses and narratives (e.g. on the pros and cons of competition); technical and scientific knowledge (especially in social science: law, economics, marketing, etc.); and competencies and skills embodied in living beings.".

[8] We are aware that we are making an oversimplification of [9] conceptualization of the market as agencement.

[9] Furthermore, the relations between the material and expressive capacities are symmetrical, meaning that each influences the other.

The second axis of the assemblage is related to the territorialization/derritorialization capacities of the parts. *Territorialization* is a process that "*increases the internal homogeneity of the assemblage*" [16] whereas deterritorialization does the opposite, decreasing the homogeneity. [10] This can relate to a spatial process, such as the difference between a face-to-face (territorialization) and a computer mediated communication (deterritorialization). But this can also be a non-spatial process. The non-spatial nature of the territorialization is what is more (but not exclusively) important for us. DeLanda argues that territorialization can be a process which excludes a certain category of people from membership of an organization. Territorialization is also a process that can reduce the heterogeneity of the possible courses of actions/relations within an assemblage. On the contrary deterritorialization is a process that can increase the heterogeneity of the possible courses of actions/relations. [45] says that we have a process in which we should observe the stabilization/consolidation (territorialization) and destabilization/dissolution (deterritorialization) of the assemblage. Indeed it is between the territorialization/deterritorialization capacities that we should be able to observe the contested space of confrontation and power postulated in [9]. We also think that, especially in sociotechnical systems such as MMORPGs, this contested space can become evident in technological breakdowns as in more traditional STS accounts (e.g. [2]; [48]).

THE ASSEMBLAGE OF CHEATING IN MMORPGS

In what follows we will describe and analyze four of the crucial elements of the cheating assemblage in MMORPGs: the game architecture, the code, the legal documents and the gameplay. We will also emphasize the material and expressive capacities and the territorialization /deterritorialization dimensions of the elements in the assemblage. The data in this paper draws upon ongoing participant observation in the MMORPG Tibia combined with data gathering and analysis of the official Tibia website and forums and the websites and forums of cheating companies. [11] In particular, we have devoted our attention to forum posts directly related to an anti-cheating campaign which has been conducted by the developer since January 2009. [12] In addition we use some empirical evidence we have collected and analysed during a pilot study on cheating in MMORPGs, that we conducted during the period September-November 2008. [13] The pilot served to identify recurrent themes in the cheating phenomenon in MMORPGs (e.g. the role of anti-cheating tools, the cheating Internet forums as centres of cheating knowledge circulation) as well as familiarizing us with the technical and colloquial vocabulary related to these games. In term of data analysis our strategy is very close to that proposed by [37] 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.

1st Element: The Game Architecture

One of the crucial elements of the cheating assemblage is the architecture of MMORPGs[14], or in other words the way in which computers involved in the game communicate and network with each other (see for an introduction [49]). The most common architecture used in MMORPGs is the master-slave, which consists of a centralized server with several clients (the players' machines) connected to it (see Figure 2). In this set-up the communication between clients involves a client sending a request to the server, the server validating, or not, the request, and then the server sending the request to all other target clients. One of the main reasons why this architecture is preferred is because by storing large part of the game execution on the server, it is possible to keep the gaming activities under control[15]: this is an expressive capacity of the infrastructure, insofar as this is just a theoretical argument in which it is postulated (for example in textbook or game networking manuals) that the master-slave is better than other choices in terms of controlling cheating[16] [32]. In addition, because the server must validate all the moves/requests made by the clients, it can also deny certain actions. Other architectures are considered less secure in terms of cheating control and in a peer-to-peer architecture (Figure 3) players depend on other players' machines for accurate information [4]. [17] The

---

[9] As it is in [24].

[10] Heterogeneity/homogeneity here does not refer to the human and non-human seamless web as it does in Actor-Network Theory. Heterogeneity refers to the variability of the elements of the assemblage.

[11] Official TIBIA forums
http://forum.tibia.com/forum/?subtopic=communityboards ; Cheating companies forums: http://www.blackdtools.com/forum/ & http://forums.tibiabot.com/

[12] These posts have been collected using the archiving software Scrapbook. Scrapbook is a Firefox extension that allows one to copy and save web pages (see http://amb.vis.ne.jp/mozilla/scrapbook/).

[13] During the pilot study we have briefly investigated some possible case studies and in particular the game World of Warcraft and the cheating forums Taultunleashed (www.taultunleashed.com) and edgeofnowhere (www.edgeofnowhere,cc). During the pilot we also have analyzed some EULAs and ToS of major MMORPGs including World of Warcarft, The Age of Conan, Runescape and Warhammer. In general we have collected some interesting data (including forums posts) and have familiarized with several MMORPGs issues.

[14] In his book [10] calls the infrastructure the "Technology of Place".

[15] Other advantages of the client-server architecture are for example the fact that it is easy to replace components and to upgrade the servers.

[16] See for example this interesting discussion
http://www.gamedev.net/community/forums/topic.asp?topic_id=377794

[17] But they might offer other advantages such as the reduction of costs

master-slave architecture is for example used in most MMORPGs including World of Warcraft (hereafter WoW). This architecture is used in Tibia too. In this way CipSoft has started a material process in which the infrastructure has a role in shaping the practice of gaming: the Tibia client must connect to one of the Tibia servers in order for the player to play the game.
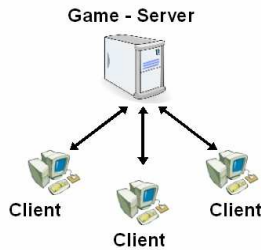

Figure 2: Master-Slave architecture

The choice of the master-slave architecture is also a clear terrritorialization in which there is an attempt to reduce the range of possible cheating actions by exercising tight control on the code's execution. In other words it is quite difficult for cheaters to, for example, modify the code of the software stored and executed on the server, whereas by contrast it is relatively easy to modify the code stored and executed on the client machine [46]. However, due to performance and scalability issues not all the game states can reside on the server. [18] As [30] have noticed "*any client-side state presents serious security risks*" (p. 10). Here the architecture seems to display also a spatial territorialization capacity in which the game resides on the company machines in centralized spaces rather than being deterritorialized onto the player's machines and spread all around the world. In technical terms this is often referred to as centralization, the idea that access, resources, and data security are controlled exclusively via the server. In fact the territorialization operated by the infrastructure is not complete and the possibility to enact cheating still remains.
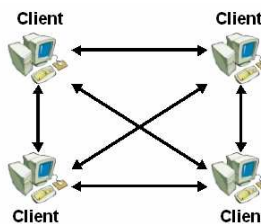

Figure 3: Peer-to-Peer architecture

The fact that some information must be stored or executed on the client machine is crucial for several types of cheats. For example, [30] describe the organization of the data structure of a MMORPG's character, and state that "*Somewhere in memory, a data structure exists that describes this character. […] Clearly these data must be stored on the game server, but sometimes the client program controls the values directly*" (p. 142). If this is the case, then an expert cheater could easily manipulate the values of a character to obtain unfair advantage. But this observation has a general validity, indeed all the game information stored on the client machine[19] or that is being manipulated and executed by the client software can, in principle, be known by cheaters and used to cheat. What follows, is a statement taken from an official Tibia article in which the company provides us with an empirical example of how the server-client balance constitutes a territorialization:

Don't you think that an **invisible creature** should be invisible for all players? We do. Hence, we will add real invisibility for monsters, something that will mainly affect players who cheated to target these creatures. Here is our message for you: Our client will not contain any information on invisible monsters anymore. It will be impossible to aim missile runes on the coordinate of an invisible creature.

Figure 4: Example of client-server balance. From [13].

This message was released by the company a few days before the release of a patch for the game (software) client. It is clear that due to cheating problems, the company decided to change the client-server balance, moving information and data on monsters previously stored on the players' machines to the server side. Indeed one of the best known features of cheating software for Tibia allows the identification of invisible creatures (see Figure 5). Again we have an attempt to reduce the possible cheating actions by a territorialization, which in this case is also spatial insofar as information on monsters is moved to the game servers.

Fishing - Automatic fishing, increased success rate
Healing - Heal yourself with spells and runes, several modes
GMs & CMs - Features helping to avoid getting banned
Fluid drinker - Drink manafluids automatically
Autoresponder - Respond automatically to messsages
Commands - Many powerfull commands with hotkeys
Light - Customizable light intensity
Invisible - Display invisible creatures, gms, cms and gods
Packet log - Log packets to make your own cheats

Figure 5: Some of the features of the Tibia cheating software BlackDProxy

---

[18] State is a concept related to the idea of finite-state machines. In terms of execution of computational processes, these processes change state often. A state refers to all the values of memory locations, registers and other component of the system that change during the execution of a process.

[19] This does not just refer to game values, [30] give the example of modifying drivers.

At the architectural level we do not just have the balance between the server and the clients, we also have to take into account the communication between these two elements. The game software can be circumvented by intercepting and/or manipulating data in real-time while in transit from the client machine to the server machine or vice versa. These types of actions are often discussed in online forums related to cheating and constitute therefore a concrete piece of the assemblage. [20] For example, the movement of a character is a type of information, or request, that goes from the client to the server. The information that goes from the client to the server can be intercepted and manipulated for cheating purposes. Often, what happen is that a proxy is put in between the server and the client in order to manipulate these communications (Figure 6). [21]
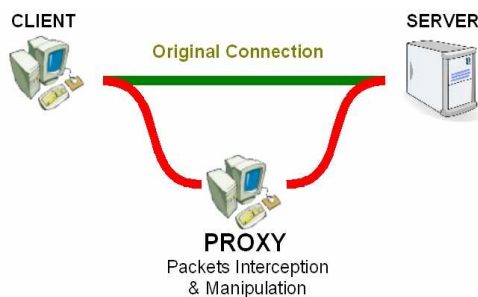

Figure 6: Proxy Operations.

In Tibia one of the main cheating tools is a proxy technology called BlackD Proxy (see http://www.blackdtools.com/blackdproxy.php). Here we witness a deterritorialization process in which the proxy changes the relations between client and server and increases the possible course of cheating actions. For example BlackD Proxy comes with a full range of different features including displaying invisible creatures, automatic fishing and healing (Figure 5).

2nd Element: The Code
Lessig [42] argues that computer code has the power to regulate the behaviour of entities in virtual worlds in a similar fashion to how legal code regulates behaviour in the real world. Indeed what we call *the code level* is an important element of the cheating assemblage in MMORPGs. There are of course a whole set of relations between the game architecture and the game code and they can be analytically distinguished, insofar they have

different roles in the assemblage. [22] The code level includes: the game client, the game executed on the server, the anti-cheating software as well as the software used by cheaters. [23] Here, mainly for reasons of space, we focus on the role of anti-cheating tools as part of the assemblage.

Several anti-cheating software solutions are used by game companies, such as *DMW anticheat*, *Punkbuster* or *Game Guard*. These anti-cheating solutions automatically enforce the terms of legal documents such as the EULA and the ToS. In this regard these tools appear to operate as material elements of more expressive elements (the legal documents): these tools enforce (punish) what legal documents discipline. [24] Anti-cheating tools also territorialize players actions. [14] proposes (although with a different goal) a similar approach in describing how different "industrial" strategies for building anti-cheating tools, participate in the definition of what is cheating by reducing the range of possible actions.
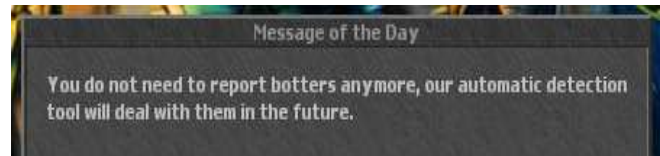

Figure 7: Introduction of the Anti-cheating tool in Tibia.

To better understand the territorialization capacity of anti-cheating tools we will briefly mention the Blizzard anti-cheating tool known as "*The Warden*". The Warden is downloaded on the fly from Blizzard servers onto users' client machines and it runs approximately every 15 seconds. The Warden is composed of small portions of code that are dynamically assembled. This means that each Warden is different from another and therefore it is difficult to create (cheating) code that can circumvent it. De facto this characteristic of the Warden makes it very difficult to create effective cheating countermeasures: here we can see how the anti-cheating tools participate in the cheating assemblage by territorializing the range of possible cheating code.

Anti-cheating tools are controversial parts of the cheating assemblage which delimit a space of confrontation and

---

[20] See here an example from edgeofnowhere forums:
http://www.edgeofnowhere.cc/viewtopic.php?p=2887795

[21] An alternative concept for understanding this process is that of *detour*, in which actors are often being forced to accept a deviation (see for example [7]; [38]) as part of the betrayal process known as *translation* [36].

[22] [14] for example does not seem to make this distinction and assumes that the architecture level is part of the code level.

[23] Cheating software solutions do not just include bots or macros, but also all possible exploitations of the game code (e.g. the exploitation of bugs or game weakness). In addition "the cheating code" relates to all the technical instruments (e.g. example hex editors or decompilers) and techniques (e.g. the reverse engineering), that can be used to manipulate the game code and for writing cheating code.

[24] In this regard often these tools appear to be similar to Digital Rights Management technologies. See for example [26].

power contestation, in Callon's terms. [25] For example, the Warden operates as a sort of spyware, scanning the RAM of player machines. [26] Among other things, the Warden searches for code on the users' machines and compares it with a dictionary of WoW know cheats code, which is maintained on Blizzard servers. It is clear here that the Warden, in a way, intervenes with a territorialization that creates a substantial boundary between detected and known cheating code and undetected code (see Figure 8).

Figure 8: The title of a thread "against" the Warden.[27]

The Warden is a key element of the cheating assemblage because it helps to understand some controversial and often contrasting power relations between the whole and the parts, for example the relations between the game company and players [5] and [50], but also the relations between the company and other entities. For example the Electronic Frontier Foundation has clearly taken a position against the Warden [21]. Greg Hoghlung, an expert security programmer and WoW player, has written a program called *the Governor* that monitors the actions of the Warden and tells the user which processes are being controlled. [28] The Governor is a process of deterritorialization[29] that aims to destabilize the territorialization operated by the Warden. [30] also provide a rich technical description on how to build cheating software, with the use of advanced rootkit techniques that inject cheating code from the kernel level rather than from the application level of operating systems. The authors claim that one of the main reasons behind the writing of this book was to counteract the controversial features of the Warden [30]. Their techniques clearly posses a deterritorialization capacity aimed at destabilizing the Warden.

---

[25] We think that is similar to what Consalvo calls as the power relationships constructed thorough code.

[26] Punkbuster, operates in a similar way, see http://www.evenbalance.com/index.php?page=info.php .

[27] From http://www.edgeofnowhere.cc/viewtopic.php?p=3764359

[28] On his website Hoghlund declares that "*Rather than debate the morality of this behavior, I would like to give the consumers the power to make this decision for themselves.*" See http://www.rootkit.com/newsread.php?newsid=371

[29] Several attempts have been made by cheating communities and companies to overcome existing anti-cheating measures. Often this becomes a goal in itself. In the case of the Warden this is quite explicit. For example WoW hackers discovered that the use of the controversial Sony Rootkit would have allowed tools made for cheating in WoW impossible to detect.

In Tibia an anti-cheating tool was introduced at the beginning of 2009. The companies that provide cheating solutions for Tibia [30] have translated their programming effort from simply providing cheating software to trying to create cheating software that is undetectable by the anti-cheating tools. From the point of view of Tibia cheating companies, the anti-cheating tool clearly operates a deterritorialization: in fact the tool has destabilized existing programming practices and market relations between these companies and cheaters [20]. To date while cheaters are asking for undetectable bots, the cheating companies appear to have failed to develop them.
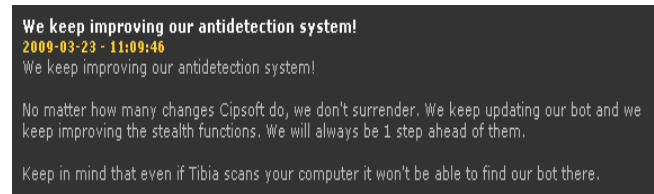

Figure 9: Working against the anti-cheating tools in Tibia.

At the same time some Tibia players fear that the new anti-cheating tool invades their privacy. This idea is not of course accepted by the whole user base. Indeed many have asked for the adoption of punkbuster or similar tools in Tibia, showing a mobilization process of other anti cheating strategies within the Tibia game forums.

Figure 10: Mobilization of other tools inside Tibia forums.[31]

However the existence of discontented players who are upset with the introduction of the anti-cheating tool in Tibia shows the fear that users often have in relation to these tools: the fear that these tools will be used not just against cheaters but also to violate the privacy of all players. Again, this shows that anti-cheating tools open up a contested space within the MMORPGs cheating assemblage, not just for cheaters but also for fair players.

---

[30] There are 2 known software companies that provide cheating software for TIBIA: blackdtools (http://www.blackdtools.com) and NG Soft (http://www.tibiabot.com).

[31] From http://forum.tibia.com/forum/?action=thread&threadid=1978162&pagenumber=30

PETITION TO STOP THE MASS-SPY ON USERS!

Figure 11: The subject of a Tibia discussion against the anti-cheating tool.[32]

3rd Element: The Textual Technologies

Textual artefacts, in particular the scientific paper and the patent, have been widely investigated in STS (see for example [47] and [6]). Texts have been described as actors that actively participate in shaping the technoscience landscape and that embody inscriptions that translate power relations [40], [2]. In this regard, software legal documents and software licenses are no exception. Software licenses constitute textual (legal) technologies [19], [35] that play an important role in shaping software users and developers practices. [33]

Several different textual documents are part of the MMORPG experience. In most cases these documents have direct relationships with the technical elements and when players install a game (software) client on their computer, they are asked to accept several documents including the EULA, the ToS[34] and often other documents such as the Game Rules or even some Privacy Agreements. [35] The acceptance of these documents is not just a user's "choice", but it is mandatory in order to play the game. It is mainly in this way that software licenses exercise their power. Indeed a license can be defined as what in Actor-Network Theory is called an *obligatory point of passage* [7]: in other words, if one would like to play the game one must accept the EULA and the ToS.

Figure 12: Detail of the WoW EULA: the user must accept the license in order to play the game.

Previously we have described the Warden anti-cheating tool which, among other things, scans the users' machines searching for cheating code in execution. Indeed, the Warden can operate on the users' machines due to a term (number 6 of the EULA) called "*Consent to Monitor*" which is inscribed into both the EULA and TOS, of WoW:

6. **Consent to Monitor.**
WHEN RUNNING, THE GAME MAY MONITOR YOUR COMPUTER'S RANDOM ACCESS MEMORY (RAM) FOR UNAUTHORIZED THIRD PARTY PROGRAMS RUNNING CONCURRENTLY WITH THE GAME. AN "UNAUTHORIZED THIRD PARTY PROGRAM" AS USED HEREIN SHALL BE DEFINED AS ANY THIRD PARTY SOFTWARE PROHIBITED BY SECTION 2. IN THE EVENT THAT THE GAME DETECTS AN UNAUTHORIZED THIRD PARTY PROGRAM, THE GAME MAY (a) COMMUNICATE INFORMATION BACK TO BLIZZARD, INCLUDING WITHOUT LIMITATION YOUR ACCOUNT NAME, DETAILS ABOUT THE UNAUTHORIZED THIRD PARTY PROGRAM DETECTED, AND THE TIME AND DATE; AND/OR (b) EXERCISE ANY OR ALL OF ITS RIGHTS UNDER THIS AGREEMENT, WITH OR WITHOUT PRIOR NOTICE TO THE USER.

Figure 13: The Consent to Monitor Term.[36]

It is by accepting the EULA, including "the consent to monitor", that players allow the Warden to scan the RAM of their machines. The licenses of other MMORPGs contain similar terms, including *Runescape* (Rule 7), *Warhammer* (EULA term 2G) and *The Age of Conan* (EULA term 5). This makes this phenomenon of licenses power even more important: the licenses exercise a power relation, insofar the players must accept the "consent to monitor" in order to play the game.

An analysis of MMORPGs legal documents is of paramount importance for the description of the cheating assemblage. Often these licenses contains terms that attempt to regulate and prevent a range of cheating practices such as the exploitation of bugs, the use of third parties software, the hacking or reverse engineering of the game code, the interception and manipulation of packets etc. Licenses can be conceived as legal code [35] and in this they are not different from computer code, insofar as they also participate in the definition of cheating by reducing the range of possible actions. Legal documents territorialize, but they do so mainly via expressive capacities, whereas the exercise of the material-territorialization capacity is delegated to anti-cheating tools or to Game Masters [14]. [37] The consent to monitor can be seen as one of the expressive elements (the laws) of the Warden (the exercise of the law).

We would like, however to emphasize another aspect of the role of legal texts in the assemblage: the discrepancy that

---

[32] From http://forum.tibia.com/forum/?action=thread&threadid=2544204

[33] From our perspective all the references to cheating in these legal texts are inscriptions that participate to the cheating assemblage.

[34] The legal documents reflect the architecture: the software that runs on the user machine falls under the EULA while the software that runs on the server falls under the protection of the ToS.

[35] See here the documents related to TIBIA http://www.tibia.com/support/?subtopic=legaldocuments ; while here there are the WoW documents http://www.worldofwarcraft.com/legal/

[36] From http://www.worldofwarcraft.com/legal/eula.html

[37] Game Masters are game company employees or expert players who are in charge of enforcing the game rules. For the role of Game Masters in TIBIA see http://www.tibia.com/gameguides/?subtopic=manual&section=support#gamemasters

exists between the expressive territorialization (i.e. the semiotic players defined in their actions by the license) and the real players that often deterritorialize/materialize cheating. For example, *The Age of Conan* Rules of Conduct states:

> You will not exploit any bug in Age of Conan and you will not communicate the existence of any such exploitable bug (bugs that grant the user unnatural or unintended benefits in game for a character of their profession and level), either directly or through public posting, to any other user of Age of Conan.

Figure 14: A term from The Age of Conan EULA.[38]

In this case the actions of the players are territorialized by the text of the license. In the term above the territorialization defines the user as a person that does not exploit bugs or does not communicate the existence of any such bugs (i.e. the possibilities for the user are reduced). However, the player often escapes the expressive/territorialization of such texts, as can be seen in the following communication of a bug in the *Age of Conan*:

> I just noticed that stamina potion in my bag is not deleted when procced. I have 4 of them total, one single and 3 stacked. When i proc single one, its not removed from bag .. which means i have unlimited amout of stamina potions (Old redrouse lvl 30). Either potion is bugged or i did something to bug it. Please check this out.
>
> From
> http://www.taultunleashed.com/phpbb2/about62122_AOC_Dupes_Unlimited_Stanima_Potions.html

It is clear here that there is a difference between the semiotic actors inscribed in the textual documents, which are not supposed to communicate the existence of bugs and the real users/players who do communicate the existence of bugs over an Internet forum. Again here we can witness a space in which there is power contestation: the licenses terms that are mandatory and imposed are not necessarily effective.

So far we have described the importance of official textual/legal documents of MMORPGs for the cheating assemblage. Cheating software, for example bots, often come with their own licenses. Some licenses are in many cases quite ordinary in their text[39] in the sense that they do not have terms that directly mention the original game they are intended to cheat/hack. Other cheating software licenses however contain interesting terms that provide us with

elements for describing the relations between providers of cheating software and the MMORPGs companies. For example, the following disclaimer comes with a WoW fishing bot called Cyberfish[40]:

> Blizzard Entertainment prohibits the use of macros or third-party utilities to automate game play to gain an unfair advantage over other players.
>
> By using this software, you hereby, release its authors of any and all liability for damages received as a direct or indirect use of this software.

As we can see the author of Cyberfish makes clear that using bots, macros or third parties software is prohibited by Blizzard. The author of the bot wants to make clear that by using the bot the cheaters release the author of the software from all liability and other problems that may arise: this license, exactly as the game official licenses, territorialize a range of possible actions. What is important to note is that both official MMORPGs legal documents and legal documents from cheating software participate in the cheating assemblage.

4th Element: The Gameplay

Gameplay constitutes a further element of the cheating assemblage. While the code and the licenses can be considered as material elements, to a large extent gameplay is an expressive element of the architecture. The situation is similar to that of the city skyline as the expressive element of the city infrastructure [28]. We do not have the intention to separate gameplay "as such" from other possibly "external" things, however it is clear that there is an analytical difference. Some interesting examples of cheating in MMORPGs are provided by [14], who refers to Social Engineering[41], or to the ability of cheaters to exploit weaknesses in the game design, or to the exploitation of soft rules that do not directly depend on the game code. In Tibia, for example, one such weakness relates to the possibility for cheaters to trap other players inside game buildings. In this way trappers can easily kill other players (in PvP servers) or get them killed by monsters (in non PvP servers).

In this section we will focus more on aspects of gameplay introduced by game developers to combat cheating. As noted by [14] designers can introduce elements in the gameplay that encourage or discourage certain actions: these elements clearly posses a territorialization capacity. In Tibia one such element is the parameter called STAMINA: "*The counter for your stamina indicates the time that is left until a character is too tired to gain experience while hunting.*".[42] This parameter has been introduced in order to

---

counteract the sharing of characters or Away From Keyboard (AFK) play. Indeed the value of this parameter is inversely proportional to the action of killing monsters. It is expected therefore that stamina can counteract the characters that are played continuously for many hours by 'sharers'[43] in order to increase their experience and level. Another of these 'soft' anti-cheating elements are the "antibot intelligent monsters". These monsters have been introduced in order to control AFK playing and while they look the same as normal creatures they heal very fast making them almost impossible to kill. So, if a (real) player encounters one of these monsters, then he/she can eventually escape from them. By contrast if the character is guided by an AFK bot, then the anti-bot monster will kill the character. Indeed, the bot will automatically attack the monsters and stick on them, without any ability to recognize whether the monster is a common or an intelligent one. A third anti-cheating element present in Tibia is a mechanism that prevents immediate disconnection while the character is engaged in fighting. This element prevents a player disconnecting while a character is being killed (either by monsters or by other players).

DISCUSSION: ASSEMBLING THE CHEATING ASSEMBLAGE

In this paper we have used some concepts from Science and Technology Studies to help us to conceptualize cheating in MMORPGs as a dynamic sociotechnical assemblage. The core idea of this approach is that a number of different elements (the architecture, the code, the licenses, the game, the gameplay, the players, the companies etc.) enter into contingent obligatory relations that create a meaningful whole. This whole is dynamic over time as territorialisation and deterritorialisation processes and expressive and material elements are contested and power relations shift. Cheating in MMORPGs cannot be defined, but rather it is contextually and historically situated. It emerges as the result of relationships that are at once empirical and historical. Socio-technical phenomena like the Warden in WoW, the anti-cheating tools in Tibia and the "consent to monitor" term in the license are clearly empirical entities that enter into historical relationships.

Our approach is multi-level, pays equal attention to technical and non-technical elements, is non-linear, focussed on relationships and involves studying a particular game over an extended period of time. We believe that this approach helps to overcome the focus in computer science and technical literature solely on technical solutions to 'prevent' cheating and on cheating as 'harmful' and the

---

[43] Away From Keyboard is an Internet slang term. In this specific case it means that the bot can play the game in place of the real player that can consequently stay Away From Keyboard.

Sharers are those players who share the same character/avatar. In this way the character can be played for long periods during the day (i.e. players/sharers play the character in turn for several hours).

overwhelming focus in media studies on players and player actions and the implied implication that cheating is positive proof of player power. For us cheating is the result of a complex range of elements and we try to avoid evaluating the behaviour as either positive or negative given that players themselves are divided on this issue.

REFERENCES

1. Achterbosch, L., Pierce, R., and Simmons, G. "Massively multiplayer online role-playing games: the past, present, and future," in *Comput. Entertain.* vol. 5, no. 4 (Mar. 2008), pp. 1-33. DOI= http://doi.acm.org/10.1145/1324198.1324207

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

3. Bardzell, J., Jakobsson M., Bardzell S., Pace T., Odom W., and Houssian A. "Virtual Worlds and Fraud: Approaching Cybersecurity in Massively Multiplayer Games," in *Situated Play, Proceedings of the DiGRA 2007* (Tokio, JP, September 2007). URL <http://www.digra.org/dl/db/07311.42219.pdf>

4. Barron T. *Multiplayer game programming*. Prima Publishing, Roseville, 2001.

5. Blizzard "A Statement on Our Hack-Scanning Process," (2005), URL < http://web.archive.org/web/20051211091852/http://forums. worldofwarcraft.com/thread.aspx?fn=blizzard-archive&t=33&p=1&tmp=1>. Accessed June 18, 2009.

6. Bowker, G. "What's in a Patent," in *Shaping Technology / Building Society: Studies in Sociotechnical Change.* Bijker, W. E. and Law, J. (Eds.)*,* MIT Press, Cambridge, Mass, 1992, pp. 53-74.

7. Callon M, "Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St Brieuc Bay," in *Power, Action, and Belief.* Law J. (Ed.), Routledge, London, 1986, pp. 196-229.

8.Callon M. '"An Essay on the Growing Contribution of Economic Markets to the Proliferation of the Social," in *Theory, Culture and Society*, vol. 24, no. 7-8, 2005, pp. 139-163.

9. Callon M. and Caliskan K. "New and Old Directions in the Anthropology of Markets," *Paper presented to Wenner Gren Foundation for Anthropological Research*, New York, 9 April, 2005.

10. Castronova E. *Synthetic worlds: The Business and Pleasure of Gaming*. Chicago University Press, Chicago, 2005.

11. Chen, B. and Maheswaran, M. "A cheat controlled protocol for centralized online multiplayer games," in *Proceedings of 3rd ACM SIGCOMM Workshop on Network and System Support For Games* (Portland, Oregon, USA, August 30 - 30, 2004). NetGames '04. ACM, New York,

NY, pp. 139-143. DOI= http://doi.acm.org/10.1145/1016540.1016554

12. CipSoft, *Where Will Cheaters Go From Here?*, January 05, 2009a, URL< http://www.tibia.com/news/?subtopic=latestnews&id=910>

13. CipSoft, *Second Patch Teaser: Stamina, Experience Counter and More,* March 05, 2009b. URL< http://www.tibia.com/news/?subtopic=newsarchive&id=945&fbegind=29&fbeginm=2&fbeginy=2009&fendd=29&fendm=3&fendy=2009&flist=11111111>

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

15. DeLap, M., Knutsson, B., Lu, H., Sokolsky, O., Sammapun, U., Lee, I., and Tsarouchis, C. "Is runtime verification applicable to cheat detection?," in *Proceedings of 3rd ACM SIGCOMM Workshop on Network and System Support For Games* (Portland, Oregon, USA, August 30 - 30, 2004). NetGames '04. ACM, New York, NY, pp. 134-138. DOI= http://doi.acm.org/10.1145/1016540.1016553

16. DeLanda M. *A New Philosophy of Society: Assemblage Theory and Social Complexity.* Continuum, London, 2006.

17. Deleuze G. and Guattari F. *A Thousand Plateaus*. Athlone, London, 1987.

18. Deleuze G. *Foucault,* Athlone, London, 1988.

19. De Paoli S., Teli M. and D'Andrea V. "Free and open source licenses in community life: Two Empirical Cases," in *FirstMonday*, vol. 13, no. 10, 6 October 2008. URL < http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2064/2030>

20. De Paoli S. and Kerr A. "The Economy of Cheating in MMORPGs," *Paper accepted for the Mediterranean Conference on Information Systems 2009 (MCIS '09)*, Athens 25-27 October, 2009.

21. Electronic Frontier Foundation. "*A new gaming feature? Spyware*," URL <http://www.eff.org/deeplinks/2005/10/new-gaming-feature-spyware> (2005), accessed 18 June, 2009.

22. Ferretti, S. and Roccetti, M. "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, November 22 - 23, 2006). NOSSDAV '06. ACM, New York, NY, pp. 1-6. DOI= http://doi.acm.org/10.1145/1378191.1378220

23. Fields, D.A. and Kafai, Y.B. " 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*, (Tokio, JP, September 2007). URL <http://www.digra.org/dl/db/07312.48067.pdf>

24. Foucault, M. *Discipline and Punish: The Birth of the Prison*. Penguin, London, 1977.

25. Galloway, A. R. *Gaming: Essays on AlgorithmicCulture*. University of Minnesota Press, Minnesota, 2006.

26. Gillespie, T. "Copyright and Commerce: The DMCA, Trusted Systems, and the Stabilization of Distribution," in *The Information Society*, vol. 20, no. 4, Sept. 2004, pp. 239-254.

27. Golle, P. and Ducheneaut, N. "Preventing bots from playing online games," *Comput. Entertain.* vol. 3, no. 3, (Jul. 2005). URL< http://doi.acm.org/10.1145/1077246.1077255>

28. Harman G. "DeLanda's ontology: assemblage and realism," in *Continental Philosophy Review*, vol.41, no. (3), 2008, pp. 367-383.

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

30. Hoglund, G. and McGraw, G. *Exploiting Online Games: Cheating Massively Distributed Systems*. First. Addison-Wesley Professional, 2008.

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

32. Kabus, P., Terpstra, W. W., Cilia, M., and Buchmann, A. P. "Addressing cheating in distributed MMOGs," in *Proceedings of 4th ACM SIGCOMM Workshop on Network and System Support For Games* (Hawthorne, NY, October 10 - 11, 2005). NetGames '05. ACM, New York, NY, 1-6. DOI= http://doi.acm.org/10.1145/1103599.1103607

33. Kücklich, J. "Homo Deludens - Cheating as a methodological tool in digital games research," in *Convergence*, vol. 13, no. 4, 2007, pp. 355-367.

34. Kücklich, J. "A Techno-Semiotic Approach to Cheating in Computer Games: Or How I Learned How to Stop Worrying and Love the Machine," in *Games and Culture*, vol. 4, no. 2, 2009, pp. 158-169.

35. Lanzara, G.F. and Morner, M., "Artifacts rule! How organizing happens in open source software projects," in *Actor-Network Theory and Organizing,* Czarniawska B. and Hernes T. (Eds.), Liber and Copenhagen Business School Press, Copenhagen, 2005, pp. 67-90.

36. Latour, B. *Science in Action, How to Follow Scientists and Engineers through Society*. Harvard University Press, Cambridge,1987.

37. Latour, B. *The pasteurization of France & Irreductions*. Harvard University Press, Cambridge, Mass, 1988.

38. Latour, B. "Morality and Technology: The End of Means," in *Theory, Culture and Society* vol. 19, no. 5/6, 2002, pp. 247-260.

39. Lash S. *Critique of Information*. Sage, London, 2002.

40. Law, J. "The Heterogeneity of Texts," in *Mapping the Dynamics of Science and Technology*, Callon M., Law J. and Rip A. (Eds.), The Macmillan press ltd., London, 1986, pp. 67-83.

41. Law J. *After Method: mess in social science research*. Routledge, London, 2002.

42. Lessig L. *Code: And Other Laws of Cyberspace*. Basic Books, New York, 1999.

43. MacBride, R., "The Primordial Economics of Cheating: Trading Skill for Glory or Vital Steps to Evolved Play," in *Situated Play, Proceedings of the DiGRA 2007*, (Tokio, JP, September 2007). URL< http://www.digra.org/dl/db/07311.05292.pdf>.

44. Mönch, C., Grimen, G., and Midtstraum, R. "Protecting online games against cheating", in *Proceedings of 5th ACM SIGCOMM Workshop on Network and System Support For Games* (Singapore, October 30 - 31, 2006). NetGames '06. ACM, New York, NY, 20. DOI= http://doi.acm.org/10.1145/1230040.1230087

45. Palmås K. "Deleuze and DeLanda: A new ontology, a new political economy?," *Paper presented the 29 January 2007 at the Economic Sociology Seminar Series*. Department of Sociology, London School of Economics.

46. Pritchard M. "How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It,", in *Gamasutra,* July 24, 2000, URL <http://www.gamasutra.com/features/20000724/ pritchard_pfv.htm>. Accessed July 12, 2009.

47. Shapin, S. "Pump and Circumstance: Robert Boyle's Literary Technology," in *Social Studies of Science*, Vol. 14, No. 4, 1984, pp. 481-520.

48. Shapin, S. and Schaffer, S. *Leviathan and the Air-Pump: Hobbes, Boyle, and the Experimental Life*. Princeton University Press, Princeton, 1985.

49. Smed J., Kaukoranta T., and Hakonen H. "Aspects of networking in multiplayer computer games," in *The Electronic Library*, vol. 20, no. 2, 2002, pp. 87-97.

50. Terdiman D. "Game players say Blizzard Invades Privacy,", in *CNET News*, 2005, URL <http://news.cnet.com/Game-players-say-Blizzard-invades-privacy/2100-1043_3-5830718.html>.

51. Yan, J. and Randell, B. "A systematic classification of cheating in online games," in *Proceedings of 4th ACM SIGCOMM Workshop on Network and System Support For Games* (Hawthorne, NY, October 10 - 11, 2005). NetGames '05. ACM, New York, NY, pp. 1-9. DOI= http://doi.acm.org/10.1145/1103599.1103606