

The Raise of the Robots in Virtual Worlds: A Comparison and a Framework for Investigating Bots in Social Networks Sites and MMOGs

Stefano De Paoli

1 Introduction and Goal of this Chapter

The goal of this chapter is to develop and discuss a comparative framework for studying bots in Virtual Worlds (VWs), focusing in particular on Social Network Sites (SNSs) and Massively Multiplayer Online Games (MMOGs).

Definitions of SNSs and MMOGs

Social Network Sites (SNSs) are platforms used by people or organisations to engage with other people and organisation and share information. According to Boyd and Ellison (2007, p. 211) they are “*web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system*”. Relevant SNSs examples are Facebook and Twitter.

Massively Multiplayer Online Games (MMOGs) are online gaming platforms often based on 3D immersive virtual environments that are played by a large number of players (Castronova, 2005; Taylor, 2006). The key goals for the players are to level their in-game persona or avatar and to engage in social interactions (e.g., forming guilds) with other players. These goals can be achieved by killing monsters or completing game quests. Relevant MMOGs examples are World of Warcraft and Eve Online.

S. De Paoli (✉)
Abertay University, Bell Street, Dundee, UK
e-mail: s.depaoli@abertay.ac.uk

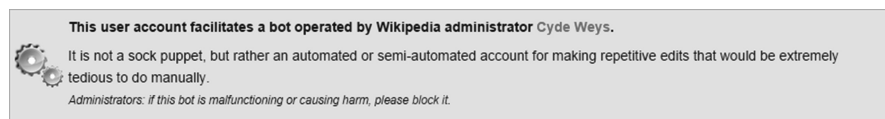


Fig. 1 Explanation of the Wikipedia bot Cydebot, from <http://en.wikipedia.org/wiki/User:Cydebot>

Bots are computer programs that automate activities for the human user over the internet. Generally bots automate activities that are seemingly repetitive and that can be time consuming to be performed manually by humans. To a certain extent therefore bots emulate and replace human activities in a variety of online contexts, especially when tasks can be easily automated due to repetition. Bots are increasingly becoming a defining component of the Internet technological and cultural landscape. According to a recent research more than 60 % of Internet traffic is generated by bots (Incapsula, 2013). Often, bots are software programs with legitimate purposes and benign functions. They can help online communities or companies in carrying out repetitive and mundane tasks. Like other forms of automation—for example workplace automation—they allow to increase productivity by automating repetitive actions. For instance, Wikipedia is largely maintained with the support of bots (Geiger, 2011) that can automate repetitive and time consuming tasks and offer a possible solution to the seemingly declining human contribution to Wikipedia (Simonite, 2013). Wikipedia bots can for example be used to revert vandalism or to make simple edits to articles. These and other activities could be repetitive and tedious if performed manually and bots are devised by editors and the community to support the maintenance of Wikipedia. Figure 1 is a description of a Wikipedia bot called Cydebot, defined as an automated or semi-automated software for making repetitive edits that would otherwise be tedious to do manually.

Another example of benign and legitimate bots are Crawling bots, such as those used by search engines. They automate the process of web pages indexing, an activity which could be extremely time consuming, repetitive and expensive if performed manually by humans. Crawling bots have been of paramount importance for the development of search engines (Sonnenreich, 1997).

While benign bots are widely diffused over the Internet, VWs are often affected by bots that have malicious intents, causing harms, disruptions and illegal activities. Malicious bots in VWs share with legitimate bots a key aspect: they are an automation of repetitive and time consuming tasks. Certain aspects of MMOGs and in particular the so called avatar levelling, can be quite repetitive—with some authors claiming that this resembles industrial repetitive work (Yee, 2006). Bots can be used to automate repetitive game actions such as killing monsters for purposes of avatar levelling. This however is a form of cheating (Consalvo, 2007; De Paoli and Kerr, 2010) and it is an explicit violation of games Terms of Services (ToSs). The use of bots for avatar levelling clearly impacts on aspects such as the VWs community, for example by polluting social relations with a proliferation of unfair achievements for cheaters. These unfair achievements can easily unbalance

the game, hence ruining the game experience for fair players. In some cases MMOGs bots are used to unfairly produce virtual assets and to accumulate virtual gold (i.e., gold-farming) that are sold over the internet for real money (an activity called Real World Trading—Heeks, 2009), again in violation of ToSs. Gold farming and the unfair accumulation of virtual assets is something that impacts on healthy and fair economic opportunities in MMOGs.

Malicious bots affect also SNSs and they are known as socialbots: automatic software able to entertain social relations (Gehl, 2013) and to build and even distort social networks (Hwang, Pearce, & Nanis, 2012), where in this second instance social networks is intended as the network of ties among social actors. Several actions of SNSs—such as awarding likes or following back other users—are also repetitive and time consuming especially in cases in which multiple accounts are used to engage with large customer bases. In SNSs, while some forms of automation are allowed or tolerated (e.g., scheduling tweets), there are bots that are used for deviant purposes such as obtaining privacy data in a deceptive way (Boshmaf, Muslukhov, Beznosov, & Ripeanu, 2011) or even intruding in organisations (Elishar, Fire, Kagan, & Elovici, 2012). Socialbots are also used to develop automatic marketing, leaning toward spam (NexGate, 2013), with the bots scraping user data and spamming users with unwanted content and advertisements. Also the use of socialbots is a violation of ToSs of SNSs.

According to official data, around 8 % of Facebook accounts could be managed by bots (Facebook, 2012) and 32 % of all tweets made by the most active Twitter users seems to be produced by bots (Sysomos, 2009). While not all of these bots have deceptive purposes, most of them have. Former research conducted on companies based in Italy, showed that bots are widely used to boost reputation and engagement on SNSs pages (Camisani Calzolari, 2012), with up to 46 % of companies followers being bots. For MMOGs we do not have the same clear data about the diffusion of bots, however it is not uncommon for game companies to ban tens of thousands (PCGAMER, 2012) or even millions of accounts linked with bots (PCGAMER, 2011). Furthermore, in both SNSs and MMOGs we have seen service providers initiating and in some cases also winning lawsuits against bot makers (Runescape, 2011; Twitter, 2012).

Given the diffusion and problems caused by malicious bots in VWs, it becomes relevant to investigate this phenomenon and develop conceptual tools for understanding the problem as well as for improving the practice. For the scope of this book, while MMOGs can be considered 3D3C Real Virtual Worlds as defined by Sivan (2008), SNSs are not. However, given the diffusion of bots in both SNSs and MMOGs and given the existence of clear similarities, a comparative research on bots in SNSs and MMOGs will strengthen our understanding on the phenomenon. This in turn will offer a greater impact on both the design and the research on 3D3C Real Virtual Worlds. Hence, the goal of this chapter is to develop an analytical-comparative framework for studying bots in SNSs and MMOGs organized around four main interconnected dimensions-concepts: automation, deception, policing

and legal definitions. This framework is the result of a multi-year qualitative research endeavour and it is the outcome of an inductive analysis process, which will be described in the next section of the chapter.

2 Methods and Concepts: The Comparative Framework for Studying Bots in VWs

The comparative framework for studying bots in SNSs and MMOGs developed in this chapter is based on empirical research and data collected over a period of 5 years by the author. This chapter also builds upon a number of previous publications by the author (De Paoli, 2013a, 2013b; De Paoli and Kerr, 2012), including a paper published in the *Journal of Virtual Worlds Research* (De Paoli and Kerr, 2009).

For MMOGs, data will come from two case studies carried out since 2009: the MMOGs *Tibia* (<http://www.tibia.com>—research started in January 2009) and *Runescape* (<http://www.runescape.com>—research started in January 2012). This includes also data coming from bot makers' websites for these games. Official documents from game developers have also been collected, including legal documents. These cases have been investigated due to the proactive approach that game companies have against bots.

For SNSs, the author conducted a research on the use of bots with a focus on studying selected socialbot makers websites and the media representation (e.g., newspaper articles) of socialbots. Also for SNSs legal documents and official communications (e.g., company's blogs) were collected and analysed. Finally, an internet marketing forum (the *Warrior Forum*—<http://www.warriorforum.com/>) has been investigated for discussions about SNSs automation. Data collection on SNSs was conducted during the year 2012 considering the following SNSs: Facebook, Twitter, Pinterest, Instagram and Soundcloud.

Finally, a note is required on the data coming from bot websites, for both MMOGs and SNSs. Many of the bot websites studied by the author are now inactive or defunct. Since VWs companies are proactive in contrasting bot makers, using for example lawsuits or aggressive technical countermeasures, bot websites are quite volatile data. When a website or a bot is defunct it will be signalled within the text of the chapter.

All the data presented in this chapter has been analysed using Grounded Theory (Charmaz, 2006) and developing a theory as outcome of data analysis. Grounded Theory is an inductive analysis technique based on the idea of coding: assigning a meaningful code (a researcher interpretation) to a portion of textual data (e.g., portions of interviews or online forum discussions). From an initial set of codes, concepts can be developed and redefined leading in advanced analysis to the development of a theory. For this research, the concepts—i.e., the dimensions of the comparative framework—are the outcome of the analysis and they have been

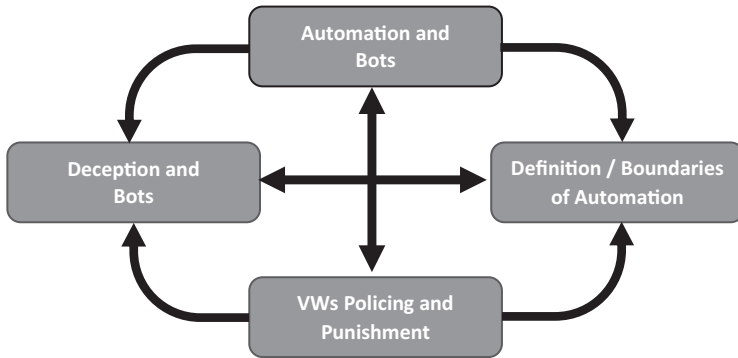


Fig. 2 The interconnected dimensions/concepts of the comparative framework for studying bots in VWs

developed initially with an open coding and then with a refinement based on both a selective coding (for the Tibia case study) and an axial coding (for Runescape and SNSs research). The conceptual framework developed in this chapter via the Grounded Theory analysis is composed of the following interconnected dimensions or concepts (see also Fig. 2):

1. Automation and bots
2. Definition of bots & Boundaries of Automation
3. VWs Policing and Punishment
4. Deception and bots

The remainder of the chapter is organised around a discussion of each dimension of the conceptual framework and their interrelations. This discussion will be substantially augmented using empirical data. For each dimension a short theoretical perspective will also be provided for greater clarity and depth, linking this research with wider debates.

3 First Dimension: Automation and Bots

Automation is the first dimension of the comparative framework for studying bots in VWs. This section shows how the concept of automation relates with bots, initially by introducing a theoretical perspective and then turning to the analysis of data.

Automation is a complex concept and it is out of the scope of this chapter to provide an exhaustive overview. A definition that can be used as starting point

comes from Marx (1976) and the chapter “*Machinery and Large Scale Industry*” of *The Capital* which offers a rich description of the process that lead to the automation of production of the manufacture system: a shift from handicraft work to its incorporation into early automatic machines. Marx’s historical-materialist account offers a clear definition of the relations between automation and work that can be used for discussing some aspects of bots. According to Marx (1976 p. 495): “*The Machine, therefore, is a mechanism that, after being set in motion performs with its tools the same operations as the worker formerly did with similar tools.*”

This definition highlights an important aspect: industrial automatic machines can replace “*human labor*” with “*machine labor*”. The machine performs the same operation of the workers with similar tools and produces output in place of the worker. In his analysis, Marx considered also some consequences of the automation of the work process, among these: (1) the deskilling of workers with their handicrafts skills being translated into machines; (2) the objectification of the production process with a reduction of workers to appendices of machineries; (3) capitalists’ use of automatic machines for increasing productivity, having need to compete with other capitalists. In the remaining of this paragraph the issues of replacement of humans with automatic machines and productivity will be further considered, whereas an account on the issues of deskilling and objectification (in relation exclusively to MMOGs bots) is offered in De Paoli (2013b) and is not considered here in-depth.

Deskilling and Bots in MMOGs

In a paper entitled *Automatic-Play and Player Deskilling*, De Paoli (2013b) introduces the concept of *Automatic-Play* in order to conceptualise the deskilling process (Braverman, 1974) that links players and bots in MMOGs.

Bots in MMOGs are automatic playing technologies that replace several of the player in-game actions. Therefore bots exhibit skills that usually belong to the human player: this includes skills related with activities such as killing monsters or looting virtual gold. What we have is properly a translation of skills (Latour, 1987) from the human actor (the player) to the non-human actor (the bot). Once a bot is launched and actively used, players/cheaters become then the supervisors of an automatic technology that possess all the skills necessary to play. This is a process of objectification of play, since play does not depend anymore on the subjective abilities of the player and depends entirely on the objective capacities of the technology. Players using bots become appendices of these technologies.

The replacement of workers with machines is a process that frees resources that can be appropriated by the capitalist, via the means of a reduction of the labour-time required to produce the same use value. Productivity is the relationship between output of goods and services (O) and the inputs (I) of the productive process:

human resources (labour), and non-human ones (such as technologies, materials and capital in general). Productivity is usually expressed as the ratio Output/Input. Productivity increases can therefore be obtained by producing more in the same time, by replacing humans with machines. Furthermore, machines can work for extended times compared to workers, without impacting the input due to an extended production time. This also leads to an increased output in linear time (i.e., more can be produced in the same amount of days).

What was just described is a conceptualization of automation that offers something for theorising bots in VWs. It is possible now to read some definitions taken from socialbot makers' websites and consider them in the light of the above discussion about automation:

Definition 1: SoundcloudRobot automates tasks you would normally do to grow your followers. (From <http://soundcloudrobot.com/about/>)

Definition 2: Manually following Instagram users in hope that they'll follow you back is a pain. Even worse is unfollowing those that don't even bother following you! Save yourself some time and let our software automate this process for you 24 h a day. Your fan base will grow every time you wake up!

(From a defunct bot for Instagram—data available at <http://web.archive.org/web/20121209042441/http://instadominate.com/>)

Definition 3: Welcome to NinjaGram, the world's #1 Instagram bot. This proprietary and versatile marketing software handles all of the repetitive grunt work, SAVES you large amounts of time, gets you thousands of followers, and helps you generate more profit from this wildly popular image sharing website! (From <http://ninjapinner.com/ninjagram-instagram-bot/>)

In these definitions, the socialbots are framed as a substitution of human labor with machines, with claims like [the bot] "*automates for you*" or "*handles the repetitive work*". And the rhetoric used, explicitly points to the idea that actions on SNSs are repetitive and time consuming, with claims like "*grunt work*" or "*manually following is a pain*". Socialbots offer a number of human action/tasks replacements that could include the following: auto-add friend, auto-commenting, auto-like/pin, auto-follow, auto-unfollow or auto-posting. This list includes most common automation features of socialbots, but should not be considered as fully exhaustive. The following example shows how these generic features are advertised on a Pinterest bot webpage:

Auto Follow feature that allows you to mass follow other users fast, gaining you thousands of followers back

Auto Unfollow function that allows you to mass unfollow users that don't follow you

Auto Pin feature that allows you to mass re-pin other images on autopilot getting you exposure

Auto Commenter feature that allows you to send out comments to all others users.

Auto like feature that allows you to mass like pins, boards, etc.

(From <http://ninjapinner.com/features/>)

All these features can, according to the bot maker, “*Get you thousands of followers on Pinterest quickly on virtual auto-pilot.*”, again an idea that points to a machine conducting the whole SNSs engagement process replacing human intervention. Therefore human actions on SNSs such as awarding likes and following are replaced by machines doing the same tasks of the user. Each of the above features provides increased output in a short amount of time: gaining followers fast, getting exposure, mass produce like or pins. Automated features of socialbots therefore allow extending a clear parallelism with automation of manufacturing: human labor tasks can be replaced with automation doing the same tasks for obtaining a greater amount of results. In the second definition (Definition 2) there is also a remark that the socialbot can operate 24 h without getting tired and easily overcoming the problem of not receiving traffic (i.e., people not following back). This allows producing results in less time compared to competitors that only work manually and therefore for few hours a day. In the third definition, the socialbot is marketed as a tool that allows to avoid “*grunt work*” while saving time and increasing followers and profit. This leads to “*massively increase*” of one’s account activity. Automation is therefore directly connected with productivity and growth of traffic on a social media accounts. This is a comment taken from a bot website, described as a “testimonial” and therefore (at least in theory) a comment from a socialbot user:

FINALLY! I am no longer spending time in front of my mobile screen doing Instagram marketing! It was a pain and I’m so glad I found this software. I’m saving countless hours each week AND I am driving in organic traffic into my website—thank you so much.

(From a defunct bot—data available at <http://web.archive.org/web/20121209042441/http://instadominate.com/>)

Again, there is the conceptualization of the socialbot as a replacement of human labor with machines (“*I am no longer spending time in front of the screen*”). The reason for adopting a socialbot lies in the repetitive and time consuming actions (“*it was a pain*”). Further, the software allows getting the same output (“*driving traffic*”) but with reduced input (“*saving time*”).

In MMOGs bots are also used to replace human activities with automation. Bot makers in MMOGs are much more sparingly offering long definitions as in the case of socialbots, however, well known bots for Runescape are for example marketed as “*leading automation for Runescape*” or as a technology that “*Emulate & automate any challenge in-game*” or as “*the ultimate automation software*”. The following are examples of descriptions of bots:

By automating the manual and repetitive aspects of the game you can set Powerbot 07 to work on any skill, task or activity and enjoy an account with high level stats and a wealth of resources.

(From <http://powerbot07.net/download/index.html>)

Our premium bots allow you to safely enjoy RS without having to go through the countless, tireless hours of developing your characters

(From a defunct bot for Runescape—data available at <https://web.archive.org/web/20100612060002/http://www.rsbots.net/runescape-bots>)

The bots in Runescape (e.g., RS) are used to perform the same repetitive and tedious tasks that a player does: the bot automates repetition for the human. The bot allows the user to “enjoy” the game, however, and this is the key aspect, the avatar levelling and development is done with substantial amount of time saved. Again automation is a way of increasing productivity, with the same output (a fully developed avatar) being readily available in short amount of time with a bot (input). Similarly to socialbots, MMOGs bots have features that are used for automation of repetitive tasks. More often these automations are specific scripts that work in conjunction with a core bot platform. In other words, the bot user purchases or downloads the core software of the bot which supports the main calls to the gaming platforms and then the user can purchase scripts tailoring the core bot software with her specific needs, e.g., a script automating fishing or a script automating harvesting. A glimpse at the scripts marketed by one of the major Runescape bot makers offers a view of the type of tasks that are automated (<http://www.powerbot.org/scripts/#premium>), some of which include: Auto fishing, Auto fire-making, Auto Magic as well as scripts that do not directly contain the word “*auto*”, but which nonetheless automate activities such as collection of loots or divination. A bot in MMOGs has therefore relevant parallel with a socialbot for SNSs as it is a replacement of human playbour (Kücklich, 2005) with automatic play (De Paoli, 2013b): an automation software carrying out the same repetitive game tasks with similar tools of players.

In both SNSs and MMOGs we have therefore a similar rhetoric surrounding productivity that the replacement of humans with technologies can achieve. We can further observe this aspect from some excerpts from forum discussions, this time taken from the MMOG Tibia:

My main point is this: bidders get high levels in a short amount [sic] of time, and because of that, they abuse of their power to either corrupt the community or break it apart.

[Posted on Tibia forum, 20/09/2008]

When some bunch of idiot kids bot 24/7 and do what took me years to accomplish in terms of magic level and level in a few weeks, that annoys the living hell out of me

[Posted on Tibia forum, 01/02/2009]

In the second case the playbour time is framed using the idea that the bot can play for extended time compared to human players. 24/7 play means that a character is played for an extensive time, not just for 1 day but often for weeks or months. We saw the issue of productivity framed in exactly the same manner in socialbot definitions (i.e., Definition 2), with the socialbot being able to operate 24 h a day. We also clearly see how players perceive bots as a threat to the community dynamics (corrupt the community) of the VW.

We can draw therefore a conclusion: that bots in VWs—be they for SNSs or MMOGs—can produce outputs (e.g., avatar levels, social engagement) for an extended time, compared to humans. This peculiar aspect allows bots to engage

and build a social network of connections or to level an avatar, while the owner of the account is not at the computer screen and while the other human competitors need to rest or attend their real life. Likewise the productivity is also enacted in a different way: the same output—a fully developed avatar or a social network of connections—can be achieved by robots in short amount of linear time.

4 Second Dimension: Bots in VWs Documents and the Boundaries of Automation

The second dimension of the comparative framework is the definitions of bots offered in official documents of VWs. These definitions set and define the boundaries of what type of automation is allowed and not allowed in VWs and why. In the previous section, bots in VWs have been characterized as automation of repetitive activities replacing human labor. However, this aspect is not different from other legal bots, for example Wikipedia bots are also meant to support a community with repetitive and time consuming tasks, allowing to maximize effort. There is something different, therefore, in malicious bots for VWs and this is the idea that increases in productivity triggered by (certain forms of) automation, create a process of unfair or unethical competition among participants. The following is a newspaper article excerpt that frames the problem in the case of Twitter:

You can't argue that the whole idea of supplementary Twitter applications is to give you distinct advantages over the official interface. You can reach followers on the other side of the planet who would normally be asleep during your active hours, you can multiply the number of actions you're capable of completing on any given day, you can live a normal life and still portray yourself as a Twitter super user, and you can use advanced filters to make it all more efficient. The question isn't whether or not it works; it's whether having access to the social networking equivalent of steroids is ethical (From <http://socialmediasun.com/twitter-ethics/>).

According to the above excerpt, the owner of a socialbot has an unethical and unfair advantage over those who do not use bots. The reason for this is that a socialbot allows the owner to reach followers and multiply activity on an account, when “purely” human competitors need to attend their normal life. An advantage which is, by analogy, comparable to the use of drugs in sport competitions (i.e., steroids). Indeed, we can imagine a situation in which two competing organisations are building a marketing campaign with SNSs, focusing on reaching potential customers and increasing traffic to a page. In this case if one organisation uses forms of automation it will be able to engage users 24/7, day and night.

That of unfair competition and the analogy of using illegal drugs in sport competition is a rhetoric that can be easily found also in MMOGs, the following is an excerpt of a forum discussion among players taken from the Tibia forum:

When someone uses a bot to hunt, it's like an athlete taking steroids.
[Posted on Tibia Forum, 01/03/2008]

Using a bot to level an avatar (i.e., hunt monsters in the above excerpt) creates unfair competition and similarly preserves the analogy of an athlete taking steroids. In MMOGs clearly players compete to reach results and the use of bots unbalance the process, with owners of bots being able to develop their avatars or to accumulate virtual assets in a short amount of linear time. This can also be achieved by using several bots controlling several puppet avatars whose virtual assets are later transferred to a main character that might be played legitimately by bot's owners.

In VWs we have rules that explicitly forbid the use of (most forms of) automation. These rules are contained in legal documents of VWs such as ToSSs, Privacy Rules, and Game Rules. This chapter does not use a legalistic perspective but a sociological and criminological perspective to consider this problem. In this perspective, a key idea is that of "social construction", a process in which social actors shape the social world around themselves and this could include social institutions, scientific knowledge and also social rules. In this perspective "criminal" or "deviant" is the act that contravenes the law or the informal norms of a social group and the definition of "right" and "wrong" is the outcome of a social construction process. Becker (1963, p. 1) in a seminal work entitled *Outsiders Studies in the Sociology of Deviance* stated: "All social groups make rules and attempt, at some time and under some circumstances, to enforce them. Social rules define situations and the kinds of behavior appropriate to them, specifying some actions as "right" and forbidding other as "wrong" ". Therefore, the definition of a deviant act does not necessarily come from abstract rules and it tends to reflect economic, cultural or political developments within the same group (Burke, 2013).

It is possible to approach the problem of the "wrong" nature of bots in VWs and therefore to understand the boundaries of what is permitted in terms of automation using the social constructivist perspective. Indeed the principles guiding the decisions about the rules may vary depending on the VWs and the actors involved. There exists for example some VWs in which automations are tolerated.

ToSSs of VWs generally forbid the use of bots, seen as a form of unfair competition over those that do not have automation and also something that ruins the experience of a game or SNSs. Furthermore, VWs often see the use of third party software application as a threat to: (1) the information security of VWs, since often they exploit weaknesses in the code or in the trust relations; or (2) to user privacy, when they are used to automatically scrape user data. Only the aspect of unfair competition will be considered further here, whereas an excellent paper on the issue of Privacy is Boshmaf et al. (2011) and the issue of trust is discussed in both Boshmaf, Muslukhov, Beznosov, & Ripeanu (2012) and De Paoli (2013a).

Different SNSs have different approaches and definitions of what is a bot or an automated software and what constitute a "wrong" action in this area. The following is a term (Tos) from the SNSs Soundcloud:

- (v) You must not employ any techniques or make use of any services, automated or otherwise, designed to misrepresent the popularity of Your Content on the Platform, or to misrepresent your activity on the Platform, including without limitation by the use of bots, botnets, scripts, apps, plugins, extensions or other automated means to register accounts, log in, add followers to your account, play Content, follow or unfollow other users, send

messages, post comments, or otherwise to act on your behalf, particularly where such activity occurs in a multiple or repetitive fashion.

(From <https://soundcloud.com/terms-of-use>)

Soundcloud is quite explicit in forbidding the use of bots and other automated software as replacement of humans (“*to act on your behalf*”). The key justification is that bots and other automated means such as macros are used with intent towards manipulating certain metrics such as the number of followers. Bots are therefore forbidden explicitly because they offer a mean to artificially increase certain outputs within the SNSs. They are explicitly declared to “*misrepresent the popularity and activity*” of an account. Pinterest also offers a similar justification (in the Acceptable use policy) stating that it is forbidden in general (and also with socialbots therefore) to:

Pin large amounts of unwanted or repetitive stuff, post unsolicited commercial messages in comments, descriptions, etc., or try to artificially boost views, Pins, comments or other metrics

(From <http://about.pinterest.com/en/acceptable-use-policy>)

Elsewhere, the author of this chapter defined this process as the *Automated Production of Reputation* (De Paoli, 2013a): the idea that aspects such as online social influence, popularity and indeed user reputation can artificially and unethically be increased with automated means. However as reputation is being manipulated with automated technologies this could lead to a breakdown of trust in VWs.

Differently from other SNSs, Twitter is much more permissive with regard to certain forms of automation and has a document called *Automation Rules and Best Practices* that states:

We’re constantly amazed by the applications and services that develop around the Twitter platform.

(From <https://support.twitter.com/entries/76915>)

Automation and third party software programs can be part of the Twitter experience as they offer solutions to problems and enhanced use of the SNS. On the same page, Twitter offers also some examples of good automation. However, the same document, right after the above sentence clarifies explicitly:

However, spammers also take advantage of automation.

(From <https://support.twitter.com/entries/76915>)

There is therefore a line that needs to be drawn between acceptable automation and automation as spam, at least in the case of Twitter. The following excerpt is again from the *Automation Rules* and is a list of automated behavior which is not allowed and considered spam:

If you have followed a large amount of users in a short amount of time;

If you have followed and unfollowed people in a short time period, particularly by automated means (aggressive follower churn);

If you repeatedly follow and unfollow people, whether to build followers or to garner more attention for your profile;

If you have a small number of followers compared to the amount of people you are following

(From <https://support.twitter.com/entries/76915>)

There are therefore explicit actions that are forbidden in general, but there is attention to actions that are done “*particularly with automated means*” as detailed in the second point of the bullet list. Twitter also set limits, some of which are public such as the limit of following no more than 1000 users per day. Other limits are instead not public, such as the calculation of ratio follower/following, which is used for calculating the total number of users that can be followed with an account (a number which is set at 2000 for newly created accounts). These limits are detailed in the document *Why Can't I Follow People?* (<https://support.twitter.com/entries/66885-i-can-t-follow-people-follow-limits>). However reversing these limits it can be concluded that automation that do not contravene the above rules is allowed. If a bot has a reasonable following pattern, it should not raise suspicions. Later in this chapter this problem will be considered further as bot makers often try to exploit these rules in order to build their automations.

MMOGs have a similar approach in defining “*right*” and “*wrong*” in relation to bots. The following term comes from the Tibia Rules:

Keep in mind that you are supposed to play the game yourself, not to have a tool or program play it for you. Doing so gives you an unfair advantage over players who invest time and effort to gain power. Using unofficial software such as a macro program or a so-called “tasker” or “bot” to automatically execute actions in Tibia for you may lead to a punishment. Thus, play fair.

(From <http://www.tibia.com/support/?subtopic=tibiarules&rule=3b>)

This term is quite descriptive compared to the more legalistic jargon of SNSs. It starts by outlining a key aspect of automation: bots are a replacement of humans with technology for playing the game. However, it is exactly this replacement that contributes to drawing the line between “*right*” and “*wrong*”: the rule states that a player is “*supposed to play the game*” and not a program. The problem of using a bot is that it offers an unfair advantage also, as human players invest time and effort to develop their avatars when instead bots can do so almost effortlessly. What follows is a Term taken from Runescape:

Software that can be used to gain an unfair advantage in our games may not be used. This includes automation tools, macros, bots, auto-typers and any other tools that circumvent any of our mechanisms designed to automatically log out inactive users.

(From http://services.runescape.com/m=rswiki/en/Macroing,_and_third-party_software)

In this case, the replacement of humans with machines is not recalled explicitly as for Tibia and the term points more directly to the problem of an “*unfair advantage*” as well as to the security issues that using a third party software may generate. It is important to outline that game ranks can also be seen as a form of (competitive) reputation system (Farmer and Glass, 2010) and using a bot to manipulate the game rank—which in both terms is the explicit justification for considering a bot

“wrong”—is again a case of *Automated Production of Reputation* (De Paoli, 2013a), with machines producing experience points that contribute to manipulated increases in the game ranks.

Analysing the data, it was possible to observe that, in SNSs in particular, the definition of what falls outside the rules in terms of automation is often connected with what constitute a “*genuine participation*” or an “*authentic interaction*”. Now these adjectives are taken directly from how SNSs define the problem. An important aspect of socialbots is that they are often marketed as technologies that create “*real*” social network of followers, versus instead networks of fake followers. This is how a bot maker frames this, over a YouTube account:

Build THOUSANDS of VERY TARGETED and REAL HUMAN FOLLOWERS in few days

(From <https://www.youtube.com/watch?v=jUv26dsu6QI>)

The idea appearing in SNSs legal documents, however, is that an interaction taking place with a socialbot or by the means of manipulated activities (e.g., likes awarded by machines, fake likes or even having a follower base of bots) is not “*authentic*”. It does not reflect what should be considered as “*genuine*”, from the view point of the service provider. Following is an excerpt from a Pinterest blog post:

Keeping Pinterest authentic is vital to helping people discover the things they love. That’s why we’ve built a dedicated spam team that has been hard at work investigating reports and building systems that detect, remove and prevent spam.

(From <http://blog.pinterest.com/post/37347668045/fighting-spam>)

Spam activities (which include bots) are an obstacle to keep authenticity in Pinterest and the owner of the platform acts with investigations and automatic systems to keep interaction authentic. The SNS here makes a clear connection between the need for an authentic experience and the policing activities that are enacted for achieving this goal. Other SNSs such as Instagram use the sentence “*genuine and meaningful interaction*” for defining the same problem. This can be found in the Instagram Community Guidelines document (<https://help.instagram.com/477434105621119/>). Facebook also clearly states the importance that connections need to be “*authentic*” and that these connections need to involve a “*real person*” and not a fake one (<https://www.facebook.com/notes/facebook-security/improvements-to-our-site-integrity-systems/10151005934870766>). Activities that tend towards manipulation and spam are against an “*authentic*” and “*genuine*” SNSs experience.

In MMOGs we do not find the idea of *authentic interaction*, mainly because interactions are not the focus of these VWs. However, bots modify the game experience for the player community in ways there are not intended by the developer: the presence of bots alter the playful atmosphere and the balance of a game. Similar rhetoric therefore can be traced in the game companies’ discussions about bots. For example early in 2009 the developer of Tibia published an article discussing its strategy against bots:

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.
(From <http://www.tibia.com/news/?subtopic=latestnews&id=910>)

The company states that it is working hard to prevent the use of bots that “*destroy the economy*” and negatively influence “*peaceful gameplay*”. We see here clearly how the company considers the negative impact of bots on both commerce and community. Even if the same words of SNSs are not used the meaning appears quite similar: there are external objects that are being used that disrupt the integrity of the MMOGs experience. Where we can find a direct connection to the idea of a “*genuine experience*” is however in the comparison between bots and humans. This is a forum post from one of the Runescape Moderators:

We will continue to evolve our anti-botting measures to hunt down those guilty of trying to spoil the game for genuine players.
(From <http://services.runescape.com/m=forum/forums.ws?294,295,84,64013824>)

A game account which is used in conjunction with a bot is not directly controlled by what is defined as a “*genuine player*”, therefore those guilty of using bots will be hunted down by the game company since they spoil the game experience. The same opposition between genuine (humans) and non-genuine (bots) players is often used in player discussion on the forums:

These bots diminish and devalue the achievements of genuine honest players.
[Posted on Runescape General Forum 07/07/2011]

Genuine players are opposed to non-genuine sorts (i.e., bots) and the latter spoil again the game experience since they diminish and devalue the achievements of the former. An idea that directly points to the problem of bots being a form of unfair competition.

In conclusion, the idea of “authentic and genuine” experience is a relevant concept for understanding the social construction of what is “*right*” and “*wrong*” in a VWs: there is a boundary between humans use of the VWs opposed to the machine use, with only the former being the one considered legitimate and authentic by the holders of legal documents.

5 Third Dimension: Policing in VWs

Directly connected with the social construction of the rules is the process of enforcing these rules. This is a third dimension of the comparative framework for studying bots in VWs. For Becker (1963, p. 122): “*enforcement of a rule is an enterprising act. Someone—an entrepreneur—must take the initiative in punishing the culprit*”. In the case of VWs, the same service provider often acts as moral entrepreneurs. They are both the holder and enforcer of legal documents.

Within VVs we have witnessed an increased use of automatic software for policing. Both SNSs and MMOGs use automatic systems for monitoring the platforms, together with a degree of human decision: the goal being the detection of bot usage and subsequent punitive actions. Facebook for example has the so called Facebook-Immune System (FIS), a technology that (Stein, Chen, & Mangla, 2011):

analyzes every action on the site as it happens, to determine its threat level, and decide how to respond. To make this decision it looks at the reputation of the cookie, IP address, and a number of other factors.

The FIS is an intrusive technology that monitors all the user actions taking place on the SNS in order to determine a threat level and take further actions. The system uses both user direct feedback (user reporting) and automatic monitoring:

the system has knowledge of aggregate patterns and what is normal and unusual. This facilitates anomaly detection, clustering, and feature aggregation.

This technology acts therefore like a panspectron (DeLanda, 1991) collecting information about everything and taking actions based on specific queries. Therefore the FIS also (but not exclusively) tries to determine socialbot activities, together with spam activities or phishing. Further, details on the functioning of the system can be found in Stein et al. (2011). Knowledge about monitoring systems for other SNSs—and especially how they work—is comparably scarce than for Facebook, but for instance both Pinterest (<http://blog.pinterest.com/post/37347668045/fighting-spam>) and Twitter (<https://support.twitter.com/entries/68916-following-rules-and-best-practices>) explicitly claim to have monitoring systems against spam. With Twitter apparently working also on real time, predictive solutions (<https://twitter.com/dickc/status/101427418832699392>).

MMOGs employ a similar strategy of policing with increased use of automatic technologies for monitoring behavior in the game (Kerr, De Paoli, & Keatinge, 2014). Both Runescape and Tibia have monitoring tools that are used for detection of bots. The following is an excerpt from a forum post from a Runescape Moderator:

Whilst I can't go into detail (as we don't want to give away any of our secrets), I can assure you we have *extremely* comprehensive macro behaviour detection tools and a dedicated team which reviews all accounts flagged before applying punishments.

[Posted on Runescape General Forum, 20/10/2010]

Therefore policing activities in MMOGs are also delegated to automatic technologies that monitor behaviors that are suspicious or are known to be possibly malicious. In both SNSs and MMOGs therefore there is a technology based on a comprehensive suspicious behavior detection that coupled with a human revision of the tool analysis could lead to application of a punishment for bot users and their accounts.

Both SNSs and MMOGs impose punishments in case of rule violations. In society, punishment has a clear social function: *“Those who break the rules benefit without contributing. They gain personal advantage by doing what the rules*

forbid.” (Cragg, 1992, p. 13). Therefore, what obtained by breaking the rules needs to be balanced back by punishment. In the case of bots this imbalance is explicitly connected with increased results due to unethical competition as well as with ruining an authentic and genuine experience.

The following is an excerpt from Tibia, and in particular an announcement of punishment:

These accounts have been identified by an automatic tool with complete accuracy, therefore any complaints about these punishments are in vain.

(From <http://www.tibia.com/news/?subtopic=newsarchive&id=921>)

The monitoring tools contribute to an accurate identification of bots and based on this a punishment is triggered. Punishments in MMOGs may vary depending on the games and are also subject to negotiations with the player community. Elsewhere (De Paoli and Kerr, 2012), the author of this chapter discussed the problem of a punishment system reform in a MMOGs, showing also how punishments for bot users might be perceived as unfair by fair players (i.e., punishments do not re-balance the harm).

The MMOGs under scrutiny here both apply temporary bans for first detection and in cases of serious-multiple violations, the permanent suspension or even the final deletion of an account. Therefore in serious cases of violations, there is no coming back to the VWs for the account. MMOGs however have different punishment systems—again something which points to a social construction process related with different cultural or economic goals—and each game might have specific arrangements, for specific situations. For example in Runescape, the use of bots may lead to reduction of the experience points of an avatar (i.e., what obtained by using a bot might be taken away—Fig. 3), whereas in Tibia this punishment does not exist (even if it was demanded by the player community).

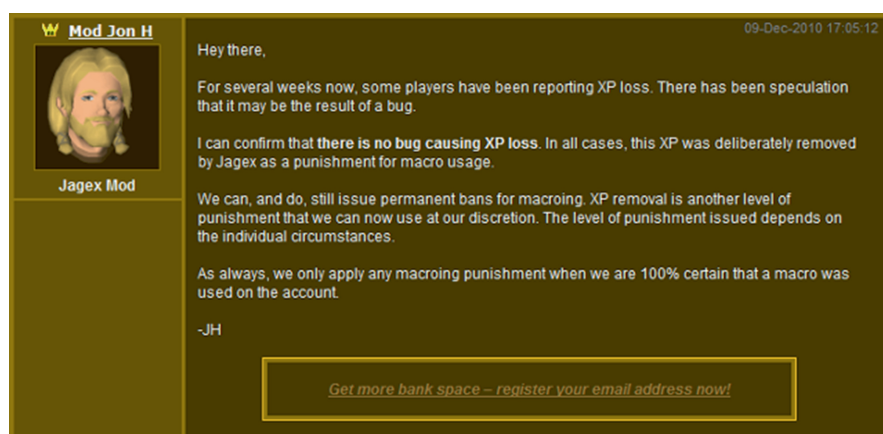


Fig. 3 One of the Runescape Moderator confirming on the forum about reduction of levels for avatars. From http://runescape.wikia.com/wiki/File:Mod_Jon_H.png

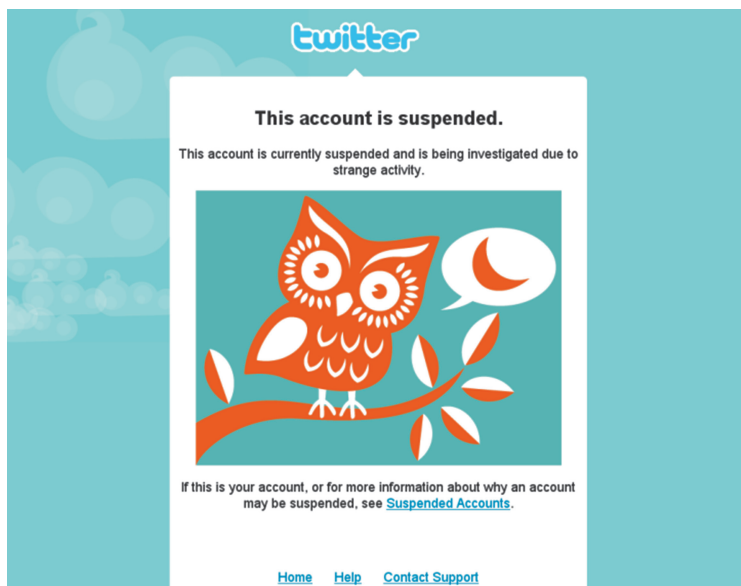


Fig. 4 Announcement of an account suspension and investigation in Twitter, for “strange activity”

Or again, in Runescape it is possible to “buy-back” for real money an account permanently suspended for the use of bots, whereas this is not possible in Tibia.

In SNSs the situation is for some aspects comparable to that of MMOGs. For example, Twitter allows certain automations but forbids others that display a spam behavior, such as aggressive following and mass unfollowing. Twitter has a clear punishment rule for this type of behavior:

Technical abuse and user abuse is not tolerated on Twitter.com, and will result in permanent suspension. Any accounts engaging in the activities specified below are subject to permanent suspension.

(From <https://support.twitter.com/entries/18311-the-twitter-rules>)

Whereof the “*activities specified below*” is the list of aggressive/automated spam behavior seen before (including the automated following churn), plus a number of other behaviors (such as the distribution of malware or pornographic material) (Fig. 4).

Therefore, the permanent suspension for an account (i.e., not coming back) is the type of punishment applied for very aggressive behavior, although this is not often directly done and Twitter offers the opportunity to discontinue abusive behavior. An example of warning, offering to discontinue abuse can be seen here: <http://blog.tweetsmarter.com/wp-content/uploads/2012/05/Chris-Loesch.png>. In some cases Twitter also issues warning, for example with flagged URLs: <https://support.twitter.com/groups/55-troubleshooting/topics/231-tweets-direct-messages/articles/90491-my-website-is-being-flagged-as-malware-or-spam>.

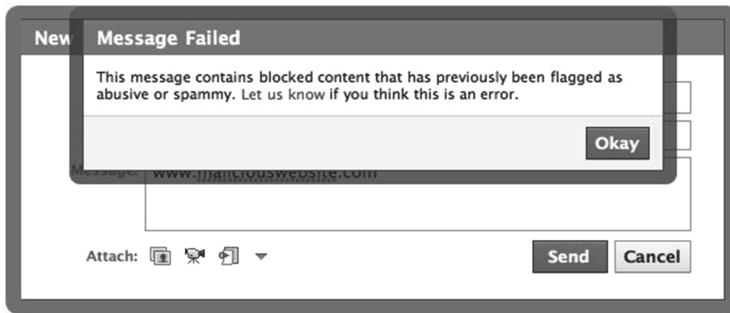


Fig. 5 Facebook warning for spam

Facebook also operates in a similar fashion. When the FIS detects the rule violation, Facebook offers initial warnings to the user, reminding them to use appropriate behavior. However, as Facebook explains:

In extreme cases where the behavior continues despite our warnings, we may disable the person's account. (From <https://www.facebook.com/notes/facebook/explaining-facebooks-spam-prevention-systems/403200567130>)

Therefore, with continuous violations, Facebook “disables” the account and again there is no coming back. This approach of SNSs is closer to the one adopted by MMOGs, which seems to have the goal of retaining customers offering them an opportunity for “redemption” from misbehavior with what in literature is defined a “forward looking” approach to punishment.

While this short excursus is not exhaustive and further research is required, it also shows a key aspect in the policing process against bots in VWs (and other violation of rules in VWs). There is initially an investigation process which is increasingly becoming automated (Kerr et al., 2014), through which secure proof of the rule violation is gathered. If the evidence is sufficient this leads to a punishment. Punishments may vary depending on VWs, but in all cases, where there are serious and multiple violations, the account might be terminated (Fig. 5).

6 Fourth Dimension: Deception and Bots

Bots in VWs disguise themselves as humans in order to remain undetectable to automatic monitoring technologies: this is the fourth dimension of the comparative framework proposed in this chapter. This is a fundamental aspect, especially in the marketing of bots as solutions for managing accounts in VWs. Indeed, while automation features are relevant, what consumers of these technologies are looking for is also a high level of “undetectability”, in order to not suffer from punishments.

Bots have clearly some resemblance with the early automations for production as detailed previously in the chapter. However, differently from “ancestor

automata”, new automatic technologies possess reception organs with which they can receive a message and take action based on that message (Wiener, 1988). In *Understanding Media*, McLuhan (1964) argues that the key aspect of the automation in the electric age is the notion of feedback: the process in which there is a dialogue between the mechanisms and its environments. This mechanism says McLuhan: “*tends to raise itself to the level of conscious awareness, so that computers seem “to think”.*” (p. 383).

Bots in VWs need to disguise themselves as humans and display to automatic monitoring technologies human-like behaviour in order to be viable in the bot market. This is necessary if bot customers are to avoid punishments. The following is an excerpt taken from the website of a (now defunct) bot:

“Why does the bot stop and count down for an hour? Instagram has hourly limits on follows, likes, and comments on a per account basis. Botstagram is not designed to break the rules of Instagram. It stays within those hourly limits, so after each account has ran, it will count down for 1 h and then start again.” (From a now defunct Instagram Bot—no URL available)

The bot operates within the limits and rules that are set by the SNSs, in order to remain undetected. In some SNSs aggressive following and other behaviors are monitored and punished. However making the bot behaving within the limits of the rules, makes the monitoring much more complex and offers to the bot user a technology which should be safe from punishments. The following is a similar excerpt from a Twitter bot, which suggests how the bot can take decisions based on external dynamics of the SNSs:

Dont Get Your Account Banned

[...]

follow and unfollow requests are done using your web browser to appear more natural

Assign different proxies for each account

Put delay on every follow and unfollow requests

Put limit to the number of users to follow

Option to not follow users that are unfollowed before

Unfollow users followed at least the specified number of days

(From the defunct web page of a Twitter bot—data available at <http://web.archive.org/web/20110411105335/http://tweetattacks.com/>)

The bot in this case offers a series of features most of all intended to comply directly with the Twitter Automation Rules. There are features meant to make an account appear natural in the behavior, such as delays in follow/unfollow, that offer opportunity for non-mechanical behavior (i.e., following someone after the same time interval) or limitations in the number of followers (limitations per day, to remain within the limit allowed by the SNSs). There is also an explicit remark that this allows to avoid punishment (*Don't Get Your Account Banned*). In forums devoted to Internet marketing (e.g., the Warrior Forum) discussions around limits of SNSs and about how to use socialbots within these limits, are quite frequent:

Remember to keep your ratio at 1:1.1 max followers/following after you pass 2000. One of the best parts of Tweet Adder is that it shows this ratio and will stop following or unfollowing at any specific ratio you set.

(From Warrior Forum: <http://www.warriorforum.com/main-internet-marketing-discussion-forum/245663-twitter-question-2001-following-limit-real-fake.html>)

This example, is extrapolated from a discussion about the ratio follower/following that one can use after he/she has reached the initial limit of 2000 following and what the SNS allows to do in term of aggressive behavior. The poster remarks a rule for appropriate ratio and offers indication for a bot (TweetAdder) that monitors this ratio. The key aspect is that socialbots need to behave within the rules in the “eyes” of monitoring technologies and actually this is a fundamental aspect for a socialbot to succeed in the market.

In MMOGs the connection between bots and deception is very comparable to SNSs: bot makers seek to develop and market technologies that behave like humans in the eyes of the monitoring technology. Actually, users are looking mainly for bots that have a high degree of undetectability in order to avoid punishment. The following excerpt is from the website of a (now defunct) bot for Tibia:

The bots are actually perfect, but none player is perfect, bots needs [sic] to make mistakes as we do, needs to “forget” some loots as I already did, “forget” to spell an exura and remember some mana after the mark [From a now removed webpage of a Tibia bot—URL not available]

There is a clear remark that the bot can act perfectly, but humans do not always act in the same manner and “*make mistakes*” and “*needs to forget*” to do things. Therefore this specific bot was programmed to act in the same manner as a human. The Tibia case study is particularly relevant since during the research, the game company introduced a brand new monitoring tool and some bots became easily detectable. After the introduction of the monitoring tools, all of the Tibia bot makers entered in a process of innovation of their technologies (De Paoli and Kerr, 2009) aimed at bringing to the market more secure bots, able to remain undetected. It is interesting to see how these new technologies were framed in the bot forums:

[the bot] will go stealth and there will be no possible counterattack for my method. Now working on adding chaos to all timers. Heal chaos done Runemaker chaos done Now working in cavebot chaos. Bot will simply act as a human.
[Posted by the bot maker on the bot Forum, 02-06-2009]

The technology of the bot therefore is improved in ways that will make the bot appear more like a human. In particular a chaos function is being introduced for making the bot act in a randomised and chaotic way, rather than in a mechanical way.

In conclusion, we can draw again a strict connection between deception in socialbots and bots in MMOGs. These technologies are developed for automation purposes, but their defining aspect is the ability to remain undetectable to existing monitoring technologies. This is necessary if bot user are to avoid punishments from VWs service providers.

7 Discussion and Conclusion: The Raise of Robots in VWs and Next Research Steps

In a *Social Media Today* article criticizing the use of automations in Social Media, McCaffrey (2011) offers—among others—this justification for avoiding automation on SNSs: “*No one wants a relationship with a robot*”, since relationships need to be among real people. This is a re-proposition of the idea of authenticity and genuine interaction discussed earlier in the chapter. However, despite the clear desire for authenticity in VWs, reality seems to be clashing with this. Indeed, already in 2011 a prediction by Gartner (2010) stated that “By 2015, 10 percent of your online ‘friends’ will be nonhuman”. We saw before that official data from Facebook are indeed close to this prediction (8 % of accounts managed by bots). Increased capabilities of socialbots (Boshmaf et al., 2011), new cutting edge research being conducted in the area of socialbot development (Hwang et al., 2012) and companies managing extensively their online presence with automated means (Camisani Calzolari, 2012), are contributing to making this prediction true. It is clear that bots are becoming a relevant aspect of the VWs experience that impacts communities, creative processes and wealth creation. Deceptive robots are on the rise in VWs. Research and scholarship in this area, therefore, are needed to explore the developments, problems and solutions to this issue.

The goal of this chapter was to propose a framework for studying bots in SNSs and MMOGs in a comparative perspective. It is the outcome of a multi-year qualitative empirical research. This framework is organised around four—deeply interconnected—concepts each pointing to a key aspect of bots: automation, deception, policing and legal boundaries of automation. While these four concepts might not necessarily be fully exhaustive of the phenomenon, they also cover a lot of ground and allow to comprehend the complexity of bots in VWs. Bots in VWs are automations that replace humans in repetitive tasks and that allow increases in productivity and outputs. These aspects however contribute to making bots a form of “*unethical and unfair competition*”, explicitly forbidden by legal documents of VWs. The existence of rules is related to their enforcement, which in VWs sees an increased use of automatic monitoring tools and different forms of punishments, all leading in the extreme case to the cessation of the account. Deception is therefore designed and implemented in bots in VWs, for avoiding both automatic monitoring and punishment.

The framework proposed in this chapter should not be considered as a theory from which to deduce provable hypotheses, rather it is more of a map that can be used for guiding future research on the subject. It is helpful for identifying trajectories and paths that might require further investigation as well as for organising existing research on the subject. Furthermore, the comparison framework is flexible enough to be used in conjunction with theories and approaches that are different from those used in this chapter: for instance the issue of legal documents could be linked with more legalistic approaches or the idea of authentic participation could be linked with existentialism (Heidegger, 1927).

From this analysis one important aspect clearly emerges: bots in MMOGs and Socialbots in SNSs converge in many ways. Each has clearly some peculiar aspects, since the latter are intended to build relations whereas the former are used to level an avatar. However, the technological framings (automation, productivity and deception) and the problems faced by VWs (legal definitions and policing) are very similar. Streams of research analysing bots in MMOGs and socialbots in SNSs need therefore to work closely together, if we are to offer appropriate research on this phenomenon.

Where to take this framework from here? The research on bots is still in its infancy in many areas. This chapter points to possible further research trajectories. For example, a research by Camisani Calzolari (2012) pointed that companies seem to use quite widely socialbots on their social media accounts. However, no extensive research to date has emerged accounting for this practice: will socialbot replace human community managers, for example? And how? Another area of investigation relates with punishment. Elsewhere, I offered an analysis of rational punishment for the MMOG Tibia. However, we do not have fully developed comparative research for both SNSs and MMOGs, in particular for the subject of bots.

References

- Becker, H. (1963). *Outsiders: Studies in the sociology of deviance*. New York: The Free Press.
- Boshmaf, Y., Muslukhov, I., Beznosov, K., & Ripeanu, M. (2011, December). The socialbot network: when bots socialize for fame and money. In *Proceedings of the 27th Annual Computer Security Applications Conference* (pp. 93–102). New York: ACM.
- Boshmaf, Y., Muslukhov, I., Beznosov, K., & Ripeanu, M. (2012, April). Key challenges in defending against malicious socialbots. In *Proceedings of the 5th USENIX Conference on Large-scale Exploits and Emergent Threats*, LEET (Vol. 12). Berkeley, CA: USENIX Association. Accessed March 15, 2014, from <https://www.usenix.org/system/files/conference/leet12/leet12-final10.pdf>
- Boyd, d. m., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210–230.
- Braverman, H. (1974). *Labor and monopoly capital: The degradation of work in the twentieth century*. New York: Monthly Review Press.
- Burke, R. H. (2013). *An introduction to criminological theory* (4th ed.). New York: Routledge.
- Camisani Calzolari, M. (2012). *Analisi sui Twitter follower delle principali aziende Internazionali*. Accessed October 12, 2014, from <http://web.archive.org/web/20130922210611/http://www.camisanicalzolari.com/MCC-Twitter-ITA.pdf>
- Castronova, E. (2005). *Synthetic worlds: The business and culture of online games*. Chicago: University of Chicago Press.
- Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. London: Sage.
- Consalvo, M. (2007). *Cheating: Gaining advantage in videogames*. Cambridge, MA: MIT Press.
- Cragg, W. (1992). *The practice of punishment: Toward a theory of restorative justice*. London: Routledge.
- De Paoli, S. (2013a). The automated production of reputation: Musing on bots and the future of reputation in the cyberworld. *International Review of Information Ethics* 19(07/2013). Accessed March 14, 2014, from <http://www.i-r-i-e.net/inhalt/019/IRIE-Paoli.pdf>

- De Paoli, S. (2013b). Automatic-play and player deskill in MMORPGs. *Game Studies*, 13(1). Accessed March 14, 2014, from http://gamestudies.org/1301/articles/depaoli_automatic_play
- De Paoli, S., & Kerr, A. (2009). "We Will Always Be One Step Ahead of Them" A case study on the economy of cheating in MMORPGs. *Journal of Virtual Worlds Research*, 2(4). Accessed March 14, 2014, from <https://journals.tdl.org/jvwr/article/view/865>
- De Paoli, S., & Kerr, A. (2010). The assemblage of cheating: How to study cheating as imbroglio in MMORPGs. *FibreCulture Journal*, (16). Accessed October 13, 2014, from <http://sixteen.fibreculturejournal.org/the-assemblage-of-cheating-how-to-study-cheating-as-imbroglio-in-mmorpgs/>
- De Paoli, S., & Kerr, A. (2012). On crimes and punishments in virtual worlds: bots, the failure of punishment and players as moral entrepreneurs. *Ethics and Information Technology*, 14(2), 73–87.
- DeLanda, M. (1991). *War in the age of intelligent machines*. New York: Zone Books.
- Elishar, A., Fire, M., Kagan, D., & Elovici, Y. (2012, December). Organizational intrusion: Organization mining using socialbots. In *Proceedings of International Conference on Social Informatics 2012* (pp. 7–12). IEEE.
- Facebook. (2012). *Quarterly report—For the quarterly period ended June 30, 2012*. Accessed March 15, 2014, from <http://www.sec.gov/Archives/edgar/data/1326801/000119312512325997/d371464d10q.htm>
- Farmer, R., & Glass, B. (2010). *Building web reputation systems*. Sebastopol, CA: O'Reilly Media.
- Gartner. (2010). *Gartner reveals top predictions for IT organizations and users for 2011 and beyond*. Accessed March 15, 2014, from <http://www.gartner.com/newsroom/id/1480514>
- Gehl, R. W. (2013). What's on your mind? Social media monopolies and noopower. *First Monday*, 18(3). Accessed March 15, 2014, from <http://firstmonday.org/article/view/4618/3421>
- Geiger, R. S. (2011). The lives of bots. In G. Lovink & N. Tkacz (Eds.), *Critical point of view: A Wikipedia reader* (pp. 78–93). Amsterdam: Institute of Network Culture.
- Heeks, R. (2009). Understanding "gold farming" and real-money trading as the intersection of real and virtual economies. *Journal of Virtual Worlds Research*, 2(4). Accessed March 15, 2014, from <http://journals.tdl.org/jvwr/index.php/jvwr/article/view/868>
- Heidegger, M. (1927). *Being and Time* (trans: Macquarrie, J., & Robinson, E., 1962). New York: Harper.
- Hwang, T., Pearce, I., & Nanis, M. (2012). Socialbots: Voices from the fronts. *Interactions*, 19(2), 38–45.
- Incapsula. (2013). *Bot traffic report*. Accessed February 15, 2014, from <http://www.incapsula.com/blog/bot-traffic-report-2013.html>
- Kerr, A., De Paoli, S., & Keatinge, M. (2014). Surveillant assemblages of governance in massively multiplayer online games: A comparative analysis. *Surveillance & Society*, 12(2), 320–336.
- Kücklich, J. (2005). Precarious playbour: Modders in the digital games industry. *FibreCulture Journal*, 5. Accessed November 12, 2009 from <http://journal.fibreculture.org/issue5/index.html>
- Latour, B. (1987). *How to write 'The Prince' for machines as well as for machination* (Online Paper). Accessed April 1, 2010, from <http://www.bruno-latour.fr/sites/default/files/36-THE-PRINCE-GB.pdf>
- Marx, K. (1976). *The capital: A critique to political economy, volume 1* (trans: Fowkes, B.) London: Penguin.
- McCaffrey, C. (2011). Four reasons why you shouldn't automate your social media marketing. *Social Media Today*. Accessed October 18, 2012, from <http://socialmediatoday.com/candacemcc/379683/four-reasons-why-you-shouldnt-automate-your-social-media-marketing>
- McLuhan, M. (1964). *Understanding media. The extensions of man* (2001 ed.). London: Routledge.
- NexGate. (2013). *The state of social media spam*. (Research Report). Accessed March 15, 2014, from <http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf>

- PCGAMER. (2011). *Runescape bot nuking event bans 1.5 million bots in one day*. Retrieved August 8, 2012, from <http://www.pcgamer.com/runescape-bot-nuking-event-bans-1-5-million-bots-in-one-day/> (Accessed 12 Oct 2014).
- PCGAMER. (2012). *Diablo 3 account bans issued to "several thousand" players using bots*. Accessed March 15, 2014, from <http://www.pcgamer.com/2012/12/19/diablo-3-account-bans-issued-to-several-thousand-players-using-bots/>
- Runescape. (2011). *Bot Busting Update Legal Proceedings*. Accessed August 8, 2012, from <http://services.runescape.com/m=news/bot-busting-update-legal-proceedings>
- Simonite, T. (2013). *The decline of Wikipedia*. Accessed June 15, 2014, from <http://www.technologyreview.com/featuredstory/520446/the-decline-of-wikipedia/>
- Sivan, Y. (2008). 3D3C real virtual worlds defined: The immense potential of merging 3D, community, creation, and commerce. *Journal of Virtual Worlds Research*, 1(1). Accessed September 16, 2014, from <https://journals.tdl.org/jvwr/index.php/jvwr/article/viewArticle/278>
- Sonnenreich, W. (1997). *A history of search engines*. Accessed March 20, 2014, from <http://www.wiley.com/legacy/compbooks/sonnenreich/history.html>
- Stein, T., Chen, E., & Mangla, K. (2011). Facebook immune system. In *Proceedings of the 4th Workshop on Social Network Systems* (pp. 1–8). New York: ACM.
- Sysomos. (2009). *An in-depth look at the 5% of most active users*. Accessed January 10, 2012, from <https://www.sysomos.com/insidetwitter/mostactiveusers/>
- Taylor, T. L. (2006). *Play between worlds: Exploring online game culture*. Cambridge, MA: MIT Press.
- Twitter. (2012). *Shutting down spammers*. Accessed March 20, 2014, from <https://blog.twitter.com/2012/shutting-down-spammers>
- Wiener, N. (1988). *The human use of human beings: Cybernetics and society*. Boston: Da Capo Press.
- Yee, N. (2006). The labor of fun how video games blur the boundaries of work and play. *Games and Culture*, 1(1), 68–71.

Handbook on 3D3C Platforms
Applications and Tools for Three Dimensional Systems
for Community, Creation and Commerce
Sivan, Y. (Ed.)
2016, XXVIII, 507 p., Hardcover
ISBN: 978-3-319-22040-6