



Between control and hacker activism: the political actions of Anonymous Brasil

Murilo Bansi Machado

Journalist, General Accounting Office, Municipality of São Paulo.
Avenida São João, 473, 16º andar
01035-000 – São Paulo – SP – Brazil
mm@murilomachado.com

Received for publication in September 2014.

Approved for publication in April 2015.

Translated by Naomi Sutcliffe de Moraes.

<http://dx.doi.org/10.1590/S0104-59702015000500002>

MACHADO, Murilo Bansi. Between control and hacker activism: the political actions of Anonymous Brasil. *História, Ciências, Saúde – Manguinhos*, Rio de Janeiro, v.22, supl., dez. 2015. Available at: <http://www.scielo.br/hcsm>.

Abstract

This paper addresses the political actions of Anonymous, the principal expression of current hacker activism, arguing that hacktivism is a form of political resistance in control societies. To this end, it focuses on studying the Brazilian, hacktivist facet of the collective. In order to stress its political character, it scrutinizes the principal expressions of hacking in the literature. It describes motivations, methods and the ethics of its political actions, based on a comparative analysis of two operations carried out by Brazilian Anonymous adherents in 2012: #OpWeeksPayment and #OpGlobo. And it finishes by identifying four of its main forms of political engagement: promotion of anonymity; “evangelization;” the formation of distributed networks; and the fact that the collective carries out and facilitates several types of political actions.

Keywords: Anonymous Brasil; hacktivism; cyber activism; control society.

Acting on the example of a network that already had a strong impact on the international community, the first nodes of the Anonymous network in Brazil began to emerge throughout the country, drawing a good deal of attention both in various social spheres and at some levels of government. Thus, this network of hacktivists established itself in a more or less coordinated way in Brazil, using the same moniker – “Anonymous” – that renewed the political hacking of a few years prior. It is important to note that the Anonymous network does not consist only of hackers. On the contrary: its supporters include activists with very distinct backgrounds, in addition to individuals connected to many different social segments, not necessarily related to hacking and technology. Without ignoring this aspect, this study focuses principally on the Brazilian hacktivist facet of this collective.

This text, based on a master’s thesis (Machado, 2013) on Anonymous in Brazil that was pioneering at the time, attempts to describe the political actions of this network, which can never be fully understood, given that the nodes and branches are rapidly and constantly changing. In it I argue that hacktivism is a form of political resistance in the context of control societies.

To this end, a descriptive case study was carried out on the principal expression of hacker activism in recent years, bringing together primary research (documentation, bibliographic research and interviews with individuals identified as involved with Anonymous Brasil) and direct observation by the researcher.

The work began with a search for the origins and principal leaders of the collective. Twenty-two people involved with Anonymous Brasil – mostly hackers – were interviewed, with two interviewed in person and the other twenty on-line. The meeting points were the communication means used by the collective, such as IRC, blogs and social networks. Additionally, reports published on sites, blogs, social networks and video and text repositories by groups and individuals identified as pertaining to Anonymous were also used.

The presence of the collective on the network was then observed during two operations undertaken by different groups that identified themselves as Anonymous in Brazil. The way in which they presented their proposals, their action methods, the communication of the collective with the public, recruitment of supporters for acts, the principal groups involved and their unavoidable contradictions were noted. In order to perform this analysis, we collected the texts posted on the two principal communication channels used during the operations – Twitter, using the on-line tool myTwebo, and IRC, by saving logs.

The following discusses the principal expressions of hacking in the literature, as well as the effects of this activity in control societies.

Hacktivism

To begin discussing the Brazilian, hacktivist facet of the Anonymous collective, we must first comment on this specific form of (cyber) activism. In the literature we can see that computer hacking has been a politically charged activity since the beginning, in the late 1950s and early 1960s.

The classic *Hackers: heroes of the computer revolution* (Levy, 2010) reveals the code of ethics, motivation and spirit of the first generation of hackers – individuals whose natural habitat

was the laboratories of the Massachusetts Institute of Technology (MIT) in the early 1960s. Levy shows that at the core of the hacker culture is the idea that information should be entirely free and that the use of computers, due to their revolutionary potential, should be as universal as possible:

Access to computers... should be unlimited and total.

All information should be free.

Mistrust authority, promote decentralization.

Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.

You can create art and beauty on a computer.

Computers can change your life for the better (Levy, 2010; emphasis in original).

The author also notes that those first computer hackers did not organize hierarchically. They were suspicious of (and sometimes mocked) authority; they promoted collaborative, decentralized actions; they shared the results of their work; and they served the community, whenever possible. Later, the hackers in what was known as the second generation – who marked the 1970s and became known as the “hardware hacker” generation – sought to change machines, making them smaller, more interactive and friendly. One of their goals was to free them from the exclusive control of specialized technicians, bringing them to the maximum number of people possible, empowering them.

Similarly to Levy, Pekka Himanen (2001) also sees traces of the political in hacking. In *A ética dos hackers e o espírito da era da informação*, the author argues that hacker ethics is in opposition to the Protestant ethic and the way of life derived from it. Comparing the principal values of the Protestant ethic (money, work, optimization, flexibility, stability, determination and accounting of results) to those of the hacker ethic (passion, freedom, social value, openness, activity, care and creativity), we note that hacking’s political positions are opposite to those of the Protestant ethic.

While hacking has always been an activity charged with political intent, one can also state that hacktivism goes one step further. While the first generations of hackers focused on policies related to software and hardware, hacktivists translated this political approach more clearly to the social plane, carrying out civil disobedience actions directly. Thus, hacker activism can be defined as the use of digital tools for exclusively political ends, often in a transgressive and/or disruptive manner. In a broader sense, it consists of a combination of the tools and technical knowledge found in hacking and a special form of political activism – carried out through digital networks (Samuel, 2004).

In this configuration, one can state that hacktivism as we know it today began in some sense in the mid-1990s, through the formation of a collaboration network to support the Zapatista movement – the “first informational guerrilla movement”¹ in history (Castells, 2002, p.103). The Zapatistas formed a large electronic military web around the Zapatista Army of National Liberation (EZLN), bringing together feminist movements, independent media groups, indigenous people, human rights activists, environmentalists and others (Clever, 1998). In addition to these traditional social movements, which also made significant use of

the Internet and other media to communicate and draw the attention of the international community (Ortiz, 2003), a small hacktivist group appeared and decided to focus their activism on the most transgressive virtual practices: Electronic Disturbance Theater – EDT (Wray, 1998).²

Since the end of the 1990s, after the EDT action, various hacktivist experiments have taken place. In 2001, however, hacking and hacktivism suffered a heavy blow. On the one hand, Antoun (2011) notes that there was a split in the hacker movement after the terrorist attacks on the Twin Towers, illustrated by a series of disagreements among participants on the Hope Conference mailing list, sponsored by the publication *2600*.³ While part of the movement wanted to answer the call of the United States Department of Defense “war on terror,” carrying out a series of attacks against totalitarian countries in an attempt to show the power of freedom of speech, another faction preferred non-aggression. This divided the movement. On the other hand, after the attacks and the implementation of the Patriot Act in the United States, which sparked a wave of surveillance worldwide, the opinion that had prevailed in government discourse and especially in the media since the 1980s became firmly established: that hackers are dangerous cybercriminals or terrorists, and hacking is an antisocial, criminal activity (Vegh, 2003).

Thus, although they still existed, hacktivist actions attempted to fly under the radar. However, this scenario changed at the end of the 2000s. With the arrival of Anonymous, a new chapter began in the story of hacker activism. Beginning in 2008, hacktivism not only began to revive, it emerged from the underground and drew so much attention that governments and corporations began to worry. Supposedly hidden by their Guy Fawkes masks, hundreds of individuals and hacktivist groups around the world have felt at liberty to perform different actions, struggling to draw the attention of the press and defy the facets of control.⁴

Control

As contemporary societies develop and adopt digital communication technologies, increasingly precise and sophisticated forms of control emerge that – through surveillance and the biopolitics of modulation – exercise a degree of control never before seen. However, the same technologies that control also provide opportunities for resistance.

When describing what is called the “control society,” Gilles Deleuze follows the example of periodization of history as carried out by Foucault and systematized by Deleuze himself (1992). Control is a stage after discipline, which in turn follows sovereignty. Foucault identified the disciplinary societies in the eighteenth and nineteenth centuries, with Napoleon Bonaparte (1769-1821) acting as the transition point between the latter and the sovereign society. There are many differences between these social systems. Deleuze continues Foucault’s work, treating power as something without central command, but affirms that the control society has even more sophisticated mechanisms to implement power, which is then exercised in the open, in a fully distributed manner, contrary to the former disciplines, which depended on the architecture of closed confinement systems.

In disciplinary societies, the language common to all means of containment is analogical. When leaving one institution to enter another (e.g. from a factory to a family, or from a school to the army), the individual is assumed to start from zero; however, in the control society, the

language common to the commands is completely numerical. Disciplinary confinement acts as a mold, disciplining individuals – the same fixed mold can be applied to various different social forms. The controls, in turn, are represented by modulation, a self-deforming mold that is adaptable, flexible, and changeable.

Discipline can be represented by a factory: placed in a mold, workers carry out similar functions, receive the same salary and negotiate collectively. But control is marked by the company: in different modulations, employees carry out different tasks, receive different salaries, and are motivated by different types of awards, bonuses etc.

In the control society, the same self-deforming modulation permeates educational training, work in a company, and family life. Control allows and encourages a real interpenetration of spaces, making individuals prisoners in the open, always traceable. For this reason, the technologies used by disciplinary societies (energetic, thermodynamic machines) give way to computing machines that also fulfill the role of helping control individuals outdoors: “The control is short-term, with rapid turnover, but also continuous and unlimited” (Deleuze, 1992, p.228).

Updating this Deleuzian formulation, authors such as Galloway (2004) noted that, in the cybernetic era, digital communication technologies became some of the control society’s principal tools, with the Internet becoming one of its greatest expressions, and hackers some of its most important political actors. After all, the new communication technologies and information networks are, above all, control technologies and networks. They allow horizontal, dispersed and distributed control. With the growing and irreversible digitization of information, combined with the unrestrained use of these technologies, every (cyber) citizen can be monitored at all times.

This monitoring can occur, principally, in two ways. The first is with respect to navigation, the implementation of cyber surveillance programs. This occurs because the social-technical networks in which we are all involved abound: business, transport, telecommunications, water, electricity, computer etc. All activities involving these networks are traceable and generate a set of data and behavior patterns that are very lucrative for typical post-industrial, capitalist institutions. Secondly, control takes place through blocking access to a variety of types of content. This includes confidential info, State secrets, and principally issues involving software, programming languages, standards, formats and protocols, all abundant on the Internet. Working with the “protocol” concept – a set of recommendations and rules that determine technical standards and, therefore, govern how “specific technologies are agreed upon, adopted, implemented and used by people throughout the world” – Galloway (2004, p.7) notes that it is useless to deny control via protocols, since one must accept one of its main protocols, TCP/IP (Transmission Control Protocol/Internet Protocol), just to navigate on the Internet. Other basic functions require new protocols, which must also be widely accepted. Therefore, fighting this form of control implies accepting it in order to push it to the limit, to elude control.

In this scenario, hacker activism appears as a response to the control society. Day after day, hacktivists join together to, among innumerable other activities: break through unwanted walls; release information of public interest; promote protection of Internet user privacy; encrypt communication; develop inclusive software, whose use does not involve

companies; and, more specifically in the case of Anonymous, carry out direct digital actions in protest against the actions of governments and/or corporations. Since it became a mass action movement, the Anons – as many Anonymous adherents call each other – have made advances against cybernetic control, pushing it to the limit.

Anonymous

Anonymous is not a group, nor a unified, formal or permanent set of individuals. It is an idea and a form of action shared by a broad, diffuse and heterogeneous network of groups and individuals. Because it is an idea, it has no owners, central leadership or geographic center. To join, you do not need permission or go through any kind of selection process.

Coleman (2011) notes that the first records of Anonymous individuals go back to 4Chan, an image forum in which users could remain unidentified. The first acts of these individuals were carried out simply “for the lulz” (lulz, an alternative form of LOL, which is an acronym for laughing out loud), that is, for fun, and were based on the principle of trolling (mockery, provocation, a kind of electronic bullying). A target became the victim of humorous and sordid attacks. On 4Chan, adherents coordinated prank telephone calls, called in multiple pizza orders for the same address, disclosed personal information, carried out DDoS actions⁵ etc. According to the researcher, Anonymous individuals carried actions of this type at least until 2006.

Two years later, in 2008, Coleman recounts that Anonymous moved “from lulz to collective action,” transforming into a collective of activists. The episode that marked this transition was a huge wave of protests against the United States Church of Scientology (Operation Chanology). The starting point was the release of a video (a practice that would become commonplace in future actions) declaring war against the institution. It also introduced another of its symbols – a faceless person wearing a dark suit, highlighting the anonymous character of the movement – and the virtual signature used by the network: “We are Anonymous. We are legion. We do not forgive. We do not forget. Expect us.” Since then, in addition to several cyber attacks, numerous posts on websites, blogs and social networks were produced to draw attention to the fact that the Church of Scientology was violating the principle of freedom of expression. At the same time, several denial of service actions against church sites were carried out. And, on February 10 of that year, several protesters involved with the issue decided to take to the streets: in various capitals of the world, more than six thousand people staged protests, especially in front of the headquarters of the Church of Scientology in North America, Europe, New Zealand and Australia (Coleman, 2011).

In 2010, Anonymous once again caught the attention of the government by triggering a larger and more complex operation, #OpPayBack, which gained momentum with the imbroglio involving the international organization Wikileaks and the companies PayPal, Mastercard and Amazon. They responded to requests by the United States government to block donations to Wikileaks (through the first two companies) and to block access to the server on which the content was hosted (Amazon).

At that time, Anonymous not only made clear their support for Wikileaks, but also decided to respond directly to the companies. For a few hours their hackers, this time also organized

through IRC,⁶ were responsible for disabling the websites of these corporations, disabling their online services and causing financial losses.

It was precisely during #OpPayBack that the first activities of Anonymous Brasil began, albeit in nascent form. Prior to that, it was not uncommon to encounter Brazilians – mostly computer hackers – acting in support of the Anonymous idea, mainly as a function of their incidental or systematic participation in the principal communication channels linked to the collective, especially 4Chan and international IRC servers. So, when the first genuinely Brazilian collectives identified with Anonymous appeared in Brazil, some of the individuals involved had already participated in operations initiated by citizens of other countries. That participation, however, was individual and sporadic, contributing mainly to specific actions.

#OpPayBack was responsible for changing this scenario. Due to its repercussions, especially after involvement in the retaliations against Wikileaks, several Brazilians sought information on participation in acts to support Anonymous. One of these privileged spaces, which played a fundamental role in the foundation of the Brazilian branch of the collective, was the forum called What is the Plan (WITP).

WITP gained momentum and adherents after Operation PayBack, when it acted as a means to answer questions and welcome new participants. After all, although many supported the mass protests triggered by the operation, most people still had no clear idea of who or what Anonymous was, or on what or how they worked. In addition to the forum, in which a Brazilian section was opened, the first IRC channels began to emerge. Inaugurated principally on the AnonOps (irc.anonops.com) and AnonNet (irc.anonnet.org) networks, these channels included direct actions, with a large number of operations and a strong dose of hactivism, in addition to other invasive and not necessarily political actions (the general case in AnonOps), and also channels whose members were also concerned with the politicization of actions and of new members (the general case in AnonNet). It is important to note, however, that these networks are extremely hybrid and, therefore, may include spaces completely outside this systematization.

With the passage of time, Brazilian Anonymous adherents began to engage in various operations, initiated spontaneously by independent groups and individuals. In constant contact with the international movement, which sometimes aided the Brazilians both with ideas for actions and with server hosting for sites and IRC, local, regional, national and even global actions were carried out, such as #OpMegaupload and the operations in support of the Arab Spring. Of them, two are analyzed in this text: #OpWeeksPayment and #OpGlobo.

The #OpWeeksPayment operation

The WeeksPayment Operation was planned and executed by the AntiSecBrTeam and iPirates groups, composed mostly of ex-members of the Brazilian branch of the LulzSec group, LulzSecBrazil. Unified behind the profile @AnonBrNews on the social network Twitter, these hackers engaged in an operation in their own way: large, showy DDoS actions, with messages through various communication channels and notices in the media. Although it was carried out between January 30 and February 3, 2012, one member of this group reported months later to the researcher that the interest in carrying it out had arisen earlier. However, they

were counseled by other individuals to not undertake it, claiming that they needed a stronger political basis and that the principal outcome would be to disrupt Brazilians during the week in which they received their paychecks.

That is because #OpWeeksPayment was precisely this: take the sites of five of the largest Brazilian banks off-line from Monday through Friday during the week on which salaries are received, when a large number of financial transactions by banks and their clients traditionally take place. Each day, one bank's server was inundated with access requests and, as a consequence, no one could reach its site. Although some sites remained off-line for a few hours, others returned within minutes, albeit with longer response times.

On Monday, January 30, the bank Itaú was the hackers' target, and its site was unstable in the morning. Tuesday was Bradesco's turn. On Wednesday and Thursday, Banco do Brasil and HSBC were affected, respectively. On Friday, the collective attacked the sites of the Brazilian Federation of Banks (Febraban), the Brazilian Central Bank, the card operators Cielo and Redecard, plus the banks Citibank, BMG and PanAmericano. On Friday (February 3), the last day of #OpWeeksPayment, the hackers made their more general objectives clear in two messages sent through the Twitter profile mentioned above: "We can cause chaos like you've never seen, but that is not the movement's objective." And then: "The goal is to alert the public about what is happening in Brazil and how it can do something to change the situation. This is what it is to be Anonymous." Although it is difficult to say if this objective was fully achieved, one can say that, at least with respect to its repercussions, the action garnered a lot of attention. Throughout the week, the hackers themselves established direct contact with the press, principally via e-mail, and released an audio message that was used by various media outlets.

For #OpWeeksPayment, the Anons involved did not require any assistance from supporters in hacker actions. In later interviews with this researcher, one of the hackers most active in #OpWeeksPayment stated more than once that, although he participates in international Anonymous operations, in hacker acts carried out by this branch "we don't need help, nor do we ask for it." However, that statement is restricted to hacking, since other forms of support are welcome and encouraged – they hope that supporters will publicize the operations and promote the political debate generated by them.

In this operation, a strong presence guiding the Brazilian Anons could still be seen: lulz, as described above. Despite claiming to be a coordinated protest with the goal of calling attention to serious political and social issues (the corruption in Brazilian political and financial systems), #OpWeeksPayment still had a playful element. Throughout the week, as the sites went off-line, group members once again used Twitter to post provocative messages. "Sailors, come see the IT team at @Itaú walking the plank! lollllol 'ItáOff' 'TangoPersonalite' 'Tango30H,'" posted the collective after the Itaú site went down, playing with two of the bank's slogans ("Itaú Personalité" and "Itaú 30h") and the expression "Tango Down," commonly used by Anons after a successful DDoS action. At the end of the operation, they posted "Internet: R\$150.00. PC: R\$1,000.00. Take down two of the largest credit card operators in the country: Priceless!", referring to Mastercard's advertising slogan.

It was also during #OpWeeksPayment that this Brazilian Anonymous group publicized one of its slogans in a very controversial way, claiming that people would hear about their

ideas “through love or pain.” In the audio message released during the operation, one of the hackers suggested that efficient protests are those capable of directly affecting people’s lives. “Our attacks were directed at government sites. But this is not having much of an effect and we saw that people were not reacting. So, we decided to take more extreme measures. They will learn about us through love or pain.” This statement caused a stir among those who, until then, were supporting #OpWeeksPayment. To them, the focus of the operations should have been to protest against the political and financial systems in Brazil, and not to inconvenience individuals.

The main complaint came from other Anonymous groups in Brazil that disapproved of the operation even before it began. Indeed, it was endlessly debated in IRC channels and on social networks. Given the anonymous, nebulous and spontaneous character of the Anonymous idea, this sort of thing is not uncommon. On the contrary, there was no record of an operation in which the planning, organization or execution methods were unanimous. During WeeksPayment, the most forceful reaction came from Plano Anonymous Brasil, a collective whose members favored the inclusive, dialogical face of Anonymous. At the time, the Twitter profile @PlanoAnonBr and the Facebook page Plano Anonymous Brasil were still active. On the second day, PlanoAnon released a statement via Facebook:

Anonymous’ target is not society. Those harmed by this action are solely and exclusively citizens, in the first week of the month, the week in which students return to school, the week when workers receive their salaries. ... This action is being carried out by @AntisecBrTeam, @iPiratesGroup and @Lulzsecbrazil, groups that openly declared themselves to be against Anonymous, and they are carrying out this action in an attempt to demoralize the collective to which we have dedicated our forces for almost one year. They, with their sick need for attention, decided to take the position that ‘if they do not respect us through love, they will respect us through pain.’

Months after the operation, various individuals participating in PlanoAnon reported to this researcher that, although it was jointly agreed that anyone could use the brand Anonymous, this did not exempt them from criticism of all types from the movement itself. And there were many: “I have nothing against any operation. If you want to attack the government, great. If you want to attack a bank, fine. But man, attacking banks on payday only affects citizens. This has a name: stupidity,” opined one of the hackers against the plan. Another individual, who collaborated with the Brazilian movement since its inception, but in actions unrelated to hacktivism, stated: “Does someone believe that taking down the site of a bank for four minutes is really going to attract people to our cause? I’d say it’s the opposite... People will increasingly see us as street urchins... troublemakers...”

However, those responsible for the protests continued. While part of the movement opposed them, not everyone did. On the third day, for example, another Facebook page, Anonymous Rio, countered the criticism:

[Anonymous] is an idea or a set of ideas continuously under construction, transformation, mutation and adaptation. There are no books, centers, groups, people or any other thing that can speak for Anonymous; each one can speak for him or herself. No one can speak for everyone. There are no leaders, and ALL MUST BE LEADERS. In short, you can be Anonymous, but you will NEVER be a member of Anonymous,

because this is not a group... What validates an operation is adhesion, pure and simple. There are no official, real or true operations, or anything like that. There are people who agree and those that don't... So if this is what we want we need to face it... And banks will continue to fall this week!

The #OpGlobo operation

The Globo Operation, carried out from April 2-10, 2012, also followed the Anonymous way of doing things: a small group of people had an idea, launched an operation and waited for potential support from Anon individuals. And, as soon as it was declared complete, its supporters disappeared and their communication channels were discontinued.

During the actions making up #OpGlobo, two of these channels stood out: the social network Twitter, via the profile created specifically for the operation (@OpGlobo), as well as several profiles of operation executors or supporters, for example @Havittaja, @AnonIRC and @AnonopsPB; and also IRC, principally through the channel #OpGlobo, created especially for this operation on the VoxAnon network (irc.voxanon.net).

Most of the posts on Twitter announced the sites that had been taken down and pointed to the IRC channel in which the conversations were taking place. Others attempted to politicize the actions through the publication of links to, for example, the documentary *Beyond Citizen Kane*, or to posters and street demonstrations against the Globo television network. The support of international Twitter profiles with very strong influence and a huge number of followers – @YourAnonNews, @Anon_Central and @AnonymousWiki – was also seen. Each of the three publicized the operation at least once.

The large number of tweets that directed Anons to the IRC led more than hundred people to #OpGlobo, a considerable number, given that the channel had been created only a short time earlier and it was the middle of a long weekend. Despite this, the channel bubbled over with messages of all types – so much so that the activity logs, for just the three main days of the operation, April 5-7, filled no less than 150 pages of a text editor with standard settings.

When reaching #OpGlobo, the first message that the user received, as in any IRC channel, was the topic. In it, the action organizers listed the target sites (to be taken down) at the time, so that whoever wanted to help them keep the pages off-line could do so, guided only by that message. However, anyone who wanted to publicize the operation or talk to those already involved in it could join the channel chat.

Those who reached the channel via a Twitter message, without having followed the operation up until then, were met with a flood of messages. During the most active days of #OpGlobo, one could observe anything from totally lost individuals to foreign hackers asking for details of the operation and offering help. The night between April 5th and 6th, for example, was animated by a rare euphoria. Even the Anons who had participated in the IRC for a while were surprised by the number of users. Before midnight, when the next target would be announced, several anxious messages appeared, with questions or suggestions. "Load the cannons!", exclaimed one Anon, followed by several others.

So when the group opted for action against the sites of the Roberto Marinho Foundation (<http://www.frm.org.br>, <http://www.fundacaorobertomarinho.com.br> and

<http://www.fundacao-robertomarinho.org.uk>), a non-governmental organization (NGO) belonging to Globo, euphoric new posts were made, either urging everyone to “attack” or reinforcing the subterfuge allegedly committed by the television network, such as the manipulation of public opinion and improper deduction of taxes through the Criança Esperança (Hope Child) project. On that day, the foundation’s page was off-line until shortly after 4 o’clock in the morning. And, as other actions were carried out, #OpGlobo participants proposed small parallel actions and, in order to undertake them, formed small groups.

In the end, Operation Globo consisted of a series of denial of service actions against several sites linked to the Globo Organization, according to a statement published in a text-sharing web application:

Hello all Anonymous associates, supporters and any other categories of people. We have begun a large operation. Tired of manipulation by Globo, we are launching #OpGlobo. Objective: sites of the subdomain: globo.com. We are relying on the help of everyone reading this message to publicize it or even help attack the websites. To make our position clear, we do not want to censure the media. The operation’s next steps will be provided via twitter (Anonymous, 2012).

In the statement, the Anons continuously updated the text as the pages went off-line, indicating the times during which they had remained inaccessible. Among those brought down, the most important were Turma da Mônica, Canal Futura, Editora Globo, Telecine, Som Livre, Globosat, Sócio Premiere and the Roberto Marinho Foundation.

#OpGlobo also continued the lulz spirit. Among the protest messages were jokes of all types. On the third day of the operation, one of the profiles posted in the microblog: “Call me the Globo Network, let me manipulate you all over, beautiful!” And, hours later: “My grandmother just fell – TANGO DOWN!:: It was Anonymous!” On IRC, during the night of the attacks, on April 6, #OpGlobo participants asked if it wasn’t a serious sin to attack someone on Good Friday.

As usual, #OpGlobo was not unanimous among Anonymous adherents. During it, a video posted on YouTube, but removed a few days later, questioned the moral and political basis of the operation. The biggest question among Anons was based on an unspoken rule, which had been followed by most of the international movement for some time: that, no matter what happened, Anonymous would not attack communication channels, even in countries in which they were controlled by the government, since this would affect freedom of information, one of the collective’s classic rallying points. “There were a lot of senseless attacks. Just attacking, with no message” – one Anon said to this researcher a few months after Operation Globo. On the maxim of not attacking the press, another Anon commented: “Initially, it would be really stupid. The press’ best weapon is contempt. The press can burn your acts, but scorning you is much worse. So attacking the press is stupid. They ignore you and you lose.”

On the other hand, #OpGlobo supporters remind us that they never attacked Globo’s news sites, and the attacks were against business sites. This was also debated via IRC: after the operation had continued for some days, some Anons suggested that the actions become more courageous, attacking the portal <http://globo.com>, for example. Immediately, one of

the organizer hackers said: “NO ATTACKS AGAINST GLOBO.COM. Globo.com is a news portal, people!” Thus, despite criticism, the protests continued and the last record of the action dates to April 10.

A short time after the Globo Operation the #OpGlobo channel on the VoxAnon network was deleted, and some of the profiles that had publicized it on Twitter were eliminated.

Political action

In prior sections, the report of the operations analyzed allowed us to observe the heterogeneous, diffuse and distributed character of Brazilian Anonymous adherents. In the following, we will highlight the principal forms of political engagement identified.

Promotion of anonymity

For Anonymous adherents, the question of anonymity is understood in different ways: as an idea, as a way to defend oneself, and as a way to engage collectively. It is the best way that the collective found to share a collective identity able to raise a legion of collaborators who did not need to be identified, prior knowledge or credentials in order to act politically. Moreover, this is one of the main strategies used to circumvent the control exercised over the networks while preserving the identity of the activists.

This anonymity interacts with a fundamental precept of hacker culture: that a hack, an action or idea should be valued for what it is, not due to the gender, ethnicity, creed, age or social position of the person who formulated it or carried it out. This was evident at various times, from the underground 4Chan to the two operations analyzed. In several of the discussions in IRC channels, whose purpose varied from proposing/assessing operations or reflecting on more immediate courses of action, many of the individuals present had no knowledge of who was behind those nicknames and, therefore, could only discuss their ideas.

In addition, the anonymity of the collective expresses another political characteristic of Anonymous: that no individual is more important than any other. Whenever an adherent tries to expand discussions beyond the idea or the cause, he tends to be marginalized. Believing that it hurts the whole principle of anonymity, much of the collective chooses to simply not work with people who act that way.

Thus, unlike the so-called “new social movements” (which include, for example, feminism, racial struggles, the fight for sexual freedom, peace and environmental movements), which are based on the social identity of their supporters, culminating in the birth of identity politics and the consequent politicization of subjectivity, identity and above all the identification process (Hall, 2005, p.45), Anonymous is based on *sui generis* identity politics. To a large extent, it does not appeal to its supporters based on their social identity, as they are very diverse. Rather, one can state that, to Anons, identity consists of relegating one's identity to the background for a time. This means that identifying with Anonymous requires adopting a collective, supposedly consensual identity to the detriment of the individuality of each supporter, which becomes hidden. Thus, note that all participate in the idea of Anonymous and, in thesis, have an active voice with respect to it. However, no one is authorized to speak on behalf of it, much less represent it.

That is why this identity is based on a dichotomy: it is weak and strong simultaneously. It is weak because it is fluid, flexible, and tenuous and there is almost no barrier to entry. But it is also strong because its conditions strongly encourage the adhesion of new supporters, even if only for one or two actions and nothing more. And, at the same time that individuals take advantage of the power of an anonymous legion to attack, they also use it to defend themselves, since anonymity facilitates even more the ability to disperse without leaving a trace – although we know that, in a cybernetic control society, this is a humanly (and mechanically) impossible task. Thus, in an era in which on-line services normally require users to register, collecting various facets of their identities to feed huge advertising databases, choosing anonymity is nonetheless a form of resistance.

It is noteworthy that, while this anonymous collective identity often tries to displace individualities, one cannot forget that it is not unifying, since it is not able (or does not try) to eliminate the diversity that characterizes the collective. So individuality is not suppressed in any way. On the contrary. Anonymous is not a homogeneous idea, nor blindly united, but rather a tangle of groups and collectives that have different thoughts and working methods, so they often conflict with each other. This can be seen in the many reactions to the WikiLeaks and Globo operations. Once proposed, while some Anons engaged in actions to support them, others disagreed on their ideology or their *modus operandi*, and criticized them openly, stimulating a debate that sometimes seems to never end. Moreover, nothing prevents those contrary to a proposal from creating their own subgroups, their own actions and their own working methods.

While choosing to hide their identities, serving a totally anonymous, diffuse collective identity, Anonymous adherents demand transparency and rigor from a large variety of governments and corporations scattered around the world – which leads to another of their unofficial slogans: transparency for them, privacy for us. In this sense, for Anons, anonymity is valid as a political tool only for those who are not in power. Any States or companies who attempt to use it for any reason are potential targets.

Evangelization

In the movements dedicated to the production, use and promotion of free software, in addition to programmers, translators (who allow a distribution or application to be used by more people all over the world), documenters (who prepare manuals and tutorials for the software) and system maintainers, there is one type of person crucial to attracting new users or collaborators: what are called “evangelists.” In general, this “evangelization” is carried out by adherents who speak well in public or who have an above-average power to convince others. For this reason, they are normally tasked by free software communities to promote their work and the movement in forums, conferences, installfests and other events. As a rule, this evangelization spreads through the network with the help of several members of these communities who post information in their blogs, social networks, or even in tools created by them expressly for promotion.

Similarly, judging by the Brazilian experience, one can say that Anonymous also engages politically, making use of some forms of evangelization – that is, promoting an idea in order to convince more people to identify with it and work towards it. However, unlike the

evangelists of free software communities, they do not often attend live events or act in the name of a group. Summarily anonymous, this work is carried out, slowly and constantly, for each operation launched, but also for the trivial day-to-day actions of the collective.

The fact is that, regardless of the group in question, the attention to evangelization seems to be an integral part of the Anonymous idea. No matter the nature of the operation, the act of evangelizing is invariably among its objectives, explicitly or implicitly. And, since it is so important and decisive, it generates a series of discussions. As mentioned above, during #OpWeeksPayment, the groups against the actions alleged that those carrying them out were not properly “evangelized.” After all, by taking down the websites of major Brazilian banks during the week salaries are paid, only bank customers were inconvenienced, so the message that the collective conveyed was inevitably distorted. On the other hand, the supporters of the operation stressed that, without attracting the attention of people and the media, no evangelization would prove effective.

Among Brazilian Anonymous adherents, this debate also extended to the methodology of the protests, as it is intimately related to how the message is conveyed – in short, to evangelization. Among the activist hackers, many said they were more in favor of defacements than denial of service actions, given that, when you disfigure the home page of a given site, you can pass a message in a much more practical and direct way than simply taking it off-line. Others, however, prefer to work with hacktivism at the level of leaking information of public interest, because this information, after disclosure, supposedly would have greater power to attract people’s attention and mobilize them. As stressed by one of the Brazilian hacktivists who has worked together with Anonymous since 2009, when questioned about the best way to evangelize: “All forms of attack only make sense if carried out at the right time. Everything has to be measured. I think that the hacktivists don’t always plan. They just do something. This is their primary error.”

Formation of distributed networks

In addition to promoting anonymity and engaging in evangelization, Anonymous also engages society politically through the formation of independent distributed networks. This (dis)organization is not without motivation: it reflects the multiplicity of individuals, ideas and methods involved in the collective and makes it, by its nature, a political actor that is very difficult (if not impossible) to defeat.

Among all of the possible definitions that differentiate centralized and decentralized networks and, as in this case, distributed networks, we chose here to follow those of the American theorist Alexander Galloway (2004, p.11-12):

A distributed network differs from other networks such as centralized and decentralized networks in the arrangement of its internal structure. A centralized network consists of a single central power point (a host), from which are attached radial nodes. The central point is connected to all of the satellite nodes, which are themselves connected only to the central host. A decentralized network, on the other hand, has multiple central hosts, each with its own set of satellite nodes ... The distributed network is an entirely different matter ... Each point in a distributed network is neither a central hub nor a satellite node – there are neither trunks nor leaves ... Like the rhizome, each node in

a distributed network may establish direct communication with another node, without having to appeal to a hierarchical intermediary.

A heterogeneous tangle of nodes directly connected to each other without hierarchical intermediaries; without control or geographical centers; in multidirectional, unrestricted communication – this is how Anonymous participants interact, a distributed network design that often relies on cells that vanish after a given operation with the same speed at which they that arose shortly before it.

Thus, in the nomadic spirit, political action in distributed networks has allowed Anonymous to develop multiple independent communities, sometimes even isolated from each other, that could follow different philosophies and work methodologies, specific objectives or the way in which they carried out actions, but respected each other's use of the name Anonymous and are intimately connected by this shared collective identity. As is pointed out above, there are many examples of these interconnected, independent communities. They form around IRC networks, channels located in these networks, social network profiles, or even while working on specific operations. These, in turn, are designed and executed in accordance with the most urgent needs and desires of those groups behind them. Only a quick visit to IRC is needed to see the surprising number of small operations occurring simultaneously, carried out by different actors.

In this way, the nature of the collective is conditioned on an intricate set of relationships – involving unions and cooperation, but also intrigues, friction, tension, contradictions, arguments etc. – that exist between these different groups, like a constantly-interacting body. As they move, undertaking new actions, publicizing new ideas, demanding new ways of acting, the collective as a whole transforms and reinvents itself – it moves from lulz to direct collective action; it moves between the network and actions on the street; and so on.

The fact that they avoid the traditional institutional forms for political action, both in protests and in decision-making, leads to Anonymous adherents being misunderstood by entities adopting hierarchical structures of organization. For example, it has become increasingly common, in mass media news, to hear of Anonymous simply as a “group” – or even as a group composed solely of hackers. In response to this, in August 2011 one Anon linked to the international movement released one of the statements that has become one of the classics of the collective, called “Anonymous is not unanimous:”

Anonymous has a perception problem. Most people think we're a group of shadowy hackers. This is a fundamental flaw. Anonymous is 'groups' of shadowy hackers, and herein lies the problem. Anonymous has done a lot of good in just the past nine months. It has helped with other groups in providing aid to people on the ground in countries where 'democracy' is a bad word. The mainstream media needs to understand that Anonymous isn't unanimous ... (Anonymous..., 2011; emphasis in original).

This is perhaps the main challenge – and also the principal concern – of the hierarchical institutions that intend to fight Anonymous. In the end, who can be blamed? Against whom can they retaliate? How can you capture an idea? How can you capture a legion? The adoption of a collective identity that constantly attempts to hide individual adherents is certainly a problem for these institutions.

Several possible political action approaches

Finally, and perhaps most importantly, one can say that Anonymous carries out and makes possible the existence and execution of a large range of political actions. This can be seen as a natural consequence of the most prominent characteristics of the collective, which have been outlined above. After all, its anonymous, distributed character, with no leadership, guidelines or geographical nucleus, allows Anonymous to attract the participation of a variety of groups and individuals in different, possibly unconnected actions that fall under the large umbrella of a faceless legion.

As noted, there are few barriers to entry for political actors who want to identify and act as Anonymous adherents. There is no need to fill out forms, follow procedural rules or send money to anyone. To a large extent, this results in a wide variety of operations, which can vary in purpose, methodology or ideology, depending on who proposed them and, especially, who adheres to them.

This vibrant plurality means that it is not costly for an individual to identify with any of the many Anon cells distributed throughout the network, or with any of the dozens of operations always taking place. And, even if this proves difficult, that individual will certainly be respected if he prefers to start his own cell or his own operation, seeking possible adherents afterward. Or in other words, Anons often gain strength through their ability to establish their own channel, profile, community, operation or movement as part of the Anonymous idea.

As a result, Anonymous has become a concrete, informal and inviting path for political engagement, culminating with a high level of activist involvement in operations with greater impact. This is because, although each of the nodes in this distributed network is dependent on the needs and wants of its support base, and changes as its foundation does, from time to time they unite in global operations that, as noted, depend on the collective work of several independent groups scattered around the world.

However, Anonymous adherents also engage politically, carrying out and facilitating political actions of all types – for example, everything from the simple act of promoting ideas through a complex hacktivist operation to disclosing sensitive information.

Final considerations

This work focused on characterizing the political action of Anonymous, identified here as the principal expression of hacker activism today. In addition, we argued that hacker activism in general and the Anonymous network in particular are set up as a form of political resistance to a specific way in which control is exercised in contemporary societies – control societies, as formulated by Deleuze (1992). Beginning with this premise, we proposed the analysis of some forms of political engagement used by groups and individuals identified with the Anonymous collective in Brazil.

Given the many actions implemented by Anons in Brazil and around the world, we noted that the collective used various tools and strategies to resist procedural control, as described by Galloway (2004) and Silveira (2012), among other authors. Their denial of service actions acted to push the control protocols to the limit, using them to block flows of communication

that serve both governments and corporations as well as network users; its radical decision to use anonymity strives to skirt control systems implemented systematically by governments and corporations throughout the world; its information leaks are a way to use the same networks employed to control them in order to show the “controllers” that they are also being observed and, at some point, will be “hacked:”

While resistance during the modern age forms around rigid hierarchies and bureaucratic power structures, resistance during the postmodern age forms around the protocological control forces existent in networks. Hacking means that resistance has changed ... Thus, it makes sense that any forces desiring to resist distributed power should themselves be adept at distributed strategies (Galloway, 2004, p.160).

Finally, the hacker activists, in their assaults on the many facets of control implemented in contemporary society, strive to call attention to new forms of political action that are increasingly revealed to be indispensable to contemporary activists. And the hacktivists, at the forefront of these movements, are seen to be critically relevant actors in political, social and economic scenarios that will continue to conform throughout this century.

NOTES

¹ In this and other citations from texts published in Portuguese, free translation is used.

² The EDT was established in 1997, with four members: Ricardo Dominguez, Brett Stalbaum, Stefan Wray and Carmin Karasic. In the 1990s, EDT carried out acts of electronic civil disobedience. It developed pioneering software, the Zapatista FloodNet, and invited several individuals to participate in mass on-line protests against the Mexican government. The application allowed people without technical knowledge to carry out distributed denial of service actions (DDoS).

³ A quarterly American periodical with content targeted towards the hacker community. The Hope Conference (an abbreviation for Hackers on Planet Earth) is currently sponsored by 2600.

⁴ Guy Fawkes was an English soldier who attempted to blow up the British Parliament during the Gunpowder Plot in 1605. Responsible for guarding the powder kegs that would be used in the explosion, he ended up being arrested and sentenced to death. This mask has become popular because of the graphic novel *V for Vendetta* by Alan Moore and David Lloyd, and principally because of the film of the same name, directed by American James McTeigue.

⁵ DDoS, or Distributed Denial of Service, is a practice that consists of accessing a given server repeatedly in order to overload it. This causes it to stop providing its services. In practice, the sites hosted on servers suffering a successful DDoS attack go off-line. The fact that it is distributed means that: (1) either various activist users access a given site uninterruptedly, generally using a specialized software that allows them to request page updates faster than a human finger could; (2) or a main computer (master) obtains control over various others (slaves), forcing them to participate in this denial of service attack. Note that DDoS does not alter the content of the pages, nor steals or damages their information. It simply disables them. For this reason, some activists prefer to call it a “protest” instead of an “attack.”

⁶ IRC is an Internet communication protocol that can be used for chatting and the exchange of small files. When Anonymous' action became more complex, involving a large number of people, several IRC servers were created so that they could be coordinated to some extent.

REFERENCES

ANONYMOUS.

Documento sobre a #OpGlobo. Paste HTML: Free anonymous HTML hosting. Disponível em: <http://pastehtml.com/raw/btg72yyul.html>. Acesso em: 15 abr. 2012. 2012.

ANONYMOUS...

Anonymous is not unanimous. Disponível em: <http://pastebin.com/4vprKdXH>. Acesso em: 15 nov. 2011. 2011.

ANTOUN, Henrique.

Expressões do novo ativismo: hackers e o individualismo colaborativo. Trabalho apresentado no Seminário Internacional Cidadania e Redes Digitais, 2011. São Bernardo do Campo. 2011.

CASTELLS, Manuel.

O poder da identidade. São Paulo: Paz e Terra. 2002.

CLEAVER, Harry.

Zapatistas e a teia eletrônica de luta. *Lugar Comum*, n.4, p.139-163. 1998.

COLEMAN, Gabriella.

Anonymous: from the lulz to collective action. *The new everyday: a media commons project*. Disponível em: <http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action>. Acesso em: 7 dez. 2011. 2011.

DELEUZE, Gilles.

Post-scriptum sobre as sociedades de controle. In: Deleuze, Gilles. *Conversações*. São Paulo: Editora34. p.223-230. 1992.

GALLOWAY, Alexander.

Protocol: how control exists after decentralization. Cambridge: MIT Press. 2004.

HALL, Stuart.

A identidade cultural na pós-modernidade. Rio de Janeiro: DP&A. 2005.

HIMANEN, Pekka.

A ética hacker e o espírito da era da informação. Rio de Janeiro: Campus. 2001.

LEVY, Steven.

Hackers: heroes of the computer revolution. Sebastopol: O'Reilly Media. 2010.

MACHADO, Murilo Bansi.

Por dentro dos Anonymous Brasil: poder e resistência na sociedade de controle. Dissertação (Mestrado em Ciências Humanas e Sociais) – Universidade Federal do ABC, Santo André. 2013.

ORTIZ, Pedro.

México rebelde. In: Coggiola, Oswaldo. *América Latina: encruzilhadas da história contemporânea*. São Paulo: Xamã. p.269-299. 2003.

SAMUEL, Alexandra Whitney.

Hactivism and the future of political participation. Tese (Doutorado em Ciência Política) – Harvard University, Cambridge. 2004.

SILVEIRA, Sergio Amadeu da.

Poder e anonimato na sociedade de controle. In: Silveira, Sergio Amadeu da; Josgrilberg, Fábio Botelho (Org.). *Tensões em rede: os limites da cidadania na internet*. São Bernardo do Campo: Universidade Metodista de São Paulo. p.109-123. 2012.

VEGH, Sandor.

Hacking for democracy: a study of the Internet as a political force and its representation in the mainstream media. Tese (Doutorado em Estudos Americanos) – University of Maryland, College Park. 2003.

WRAY, Stephen.

Electronic civil disobedience and the world wide web of hacktivism: a mapping of extraparliamentarian direct action net politics. *Switch: New Media Journal*, v.4, n.2. Disponível em: <http://switch.sjsu.edu/web/v4n2/stefan/index.html>. Acesso em: 3 fev. 2012. 1998.

