

### Guiomar Rovira Sanch

(Universidad Autónoma Metropolitana)

[grovira@correo.xoc.uam.mx]

DOI: https://dx.doi.org/10.12795/IC.2019.i19.03

E-ISSN: 2173-1071

IC – Revista Científica de Información y Comunicación 2019, 16, pp. 85 – 127

#### Abstract

Contentious collective action has been transformed in the last three decades. Social movements, in their great diversity, have promoted innovative and unexpected ways of using Information and Communication Technologies. Each wave of communicative power oriented to emancipatory action, that is, of technopolitics for collective self-determination and deliberation, has been followed by another of corporate interference and control, that is, of technopolitics that seaks the interest of powerfull instances and capital. Contrasting the hacktivist tactics of the connected multitudes with the proliferation of networked marketing and counterinsurgency strategies implies reflecting on means and ends in the era of digital and data colonialism.

#### Resumen

La acción colectiva contenciosa se ha transformado en las tres últimas décadas. Los movimientos sociales, en su gran diversidad, han impulsado propuestas innovadoras y usos de las Tecnologías de la Información y la Comunicación insospechados. A cada ola de potencia comunicativa orientada a la acción emancipatoria, es decir, de tecnopolítica para la autodeterminación colectiva y la deliberación, le ha seguido otra de injerencia corporativa y de control, es decir, de tecnopolítica determinante desde los intereses del poder y del capital. Contrastar las tácticas hacktivistas de las multitudes conectadas con la proliferación de estrategias de marketing y de contrainsurgencia en red, implica refiexionar sobre medios y flnes en la era del colonialismo digital y de datos.

### Keywords

Technopolitics, netwar, hacktivism, fake news, connected crowds, counterinsurgency.

#### Palabras clave

Tecnopolítica, guerra de red, hacktivismo, fake news, multitudes conectadas, contrainsurgencia

### Summary

- 1. Introduction
- 2. Techno-politics, freedom and war on the Web
- 3. The means and the ends. Hacker method vs. authority/author/authorised
- 4. The advent of hacktivism and the conquest of cyberspace
- 5. The splendour of emancipatory techno-politics: connected multitudes
- 6. Determining techno-politics: terrorism and the ultra-right
- 7. The feminist wave and violent regression
- 8. The state and the netwar
- 9. Digital colonialism and technological dependence
- 10. Resistance is life: the exploit
- 11. Counter-insurgency and widespread humiliation
- 12. Rails over the sea
- 13. Bibliography

#### Sumario

- 1. Introducción
- 2. Tecnopolítica, libertad y guerra en la red
- 3. Medios y flnes. Método hacker vs autoridad/autor/autorizado
- 4. El advenimiento del hacktivismo y la toma del ciberespacio
- 5. El esplendor de la tecnopolítica de emancipación: las multitudes conectadas
- 6. Tecnopolítica de determinación: terrorismo y ultraderecha
- 7. La ola feminista y la regresión violenta
- 8. El Estado y la guerra en la red
- 9. El colonialismo digital y la dependencia tecnológica
- 10. La resistencia es la vida: el exploit
- 11. Contra insurgencia y humillación generalizada
- 12. Rieles sobre el mar
- 13. Bibliografía

## 1. Introduction

Only war makes it possible to mobilize all of today's technical resources
while maintaining the property system.
Walter Benjamin

Contentious collective action has been transformed in the last three decades. Social movements, in their great diversity, have promoted innovative and unexpected ways of using information and communication technologies (hereinafter ICTs). Each wave of communicative power aimed at emancipatory action, that is, techno-politics for collective self-determination, has been followed by another of corporate interference and control, namely, of decisive techno-politics.

In this paper, I examine the two sides of techno-politics in the Digital Era, the most democratising and the most coactive, from utopian to the most dystopian reflections on the Internet. My analysis is based on a systematic and situated monitoring of the communication production of Mexican and Spanish social movements. Feminist epistemology claims that

there is no place from which it is possible to develop knowledge free from values and prejudices, but some positions are better than others, and that the ideal epistemic agent is not an unconditioned subject, but a subject conditioned by social experiences (Blazquez, 2010, p. 30).

In my case, I have accompanied social mobilisation processes in my hometown of Barcelona since the mid-1980s, the Zapatista movement in Mexico as of 1994, connected multitudes like the Spanish 15-M and the Mexican #YoSoy132 movements and their developments in the past few years, plus the multiple social movements that have emerged in Latin America up until the current global wave of feminist demands (Rovira, 2009, 2017, 2018).

I propose to distinguish between two ways of appropriating the Internet and ICTs: on the one hand, emancipatory or self-determining techno-politics and, on the other, coactive or decisive techno-politics. The former corresponds to a techno-political reflection arising from social mobilisation processes like the Spanish 15-M movement that occupied the squares demanding a deeper democracy, defined by Toret (2013) as 'the

re-appropriation of digital tools and spaces to create moods and common notions central to empowerment, in order to enable collective behaviours in the urban space that lead to taking the reins of common issues' (p. 45).

The second corresponds to what the author calls the 'the new 1 per cent techno-political machines' (Toret, 2019), to wit, the leveraging of digital networks by companies, interest groups, states and political parties with specific aims—in many cases obscure, but not necessarily so. Their purpose is not to encourage people 'to take the reins of common issues', but to make them accept 'the particular issues' that are proposed to them, whether it be purchasing a product, casting their vote or reinforcing their identity.

The many post-foundational political philosophers (Marchart, 2007), from Arendt (1993) and Schmitt (1993) to Rancière (1996), Badiou (1999) and Laclau (2005), define the difference between the political sphere and the political. In other words, between politics as the management of what has been established in a specific distribution of power and the political as an open development that interferes in the rules and generates a potential for instituting quality.<sup>2</sup>

In this connection, decisive techno-politics corresponds to the duration and quest for the continuity of a social system and a distribution of power through strategies,<sup>3</sup> which can be commercial, political or warlike. On the other hand, self-determining or emancipatory techno-politics, as a development, interrupts or disrupts the continuity of that system at a given moment, challenging that distribution of (material and symbolic) power

- In Post-Foundational Political Thought, Oliver Marchart explains, 'the political (located, as it were, on the "ontological" side of Being-as-ground) will never be able fully to live up to its function as Ground and yet it has to be actualized in the form of an always concrete politics that necessarily fails to deliver what it has promised' (2007, p. 8, emphasis added).
- 2 Each author defines this difference in his or her own words. For instance, Arendt speaks of the political vs. the social; Rancière of the political vs. the police; Castoriadis of the instituted vs. the instituting; etc.
- 3 What Michel de Certeau calls 'strategy' is 'the calculus of force-relationships which becomes possible when a subject of will and power (a proprietor, an enterprise, a city, a scientific institution) can be isolated from an "environment" (1984, p. xix), a place where he 'can capitalize on its advantages, prepare its expansions, and secure independence with respect to circumstances.' (1984, p. xix).

using prefigurative tactics<sup>4</sup> (Certeau, 1984) and practices that reveal 'other possible worlds'.

AUTO-DETERMINING TECHNO-POLITICS	DECISIVE TECHNO-POLITICS
Undetermined open development	Determined induced development
Collectively self-managed	Group-managed
Active/creative potential	Coactive/instrumental potential
Fosters the commons and the cosmopolitan (logic of 99 per cent vs. 1 per cent)	Fosters the private and the identity-related (logic of profit and of friend vs. enemy)
Tactics	Strategies
Frames of motivation: delight in diversity. The commons to be constructed	Frames of motivation: fear and defence of identity. One's own threatened

This classification is a tool for analysing the coexistence of these techno-political aspects since the very beginnings of computational research. Weber (1978 [1968]) notes, 'As in the case of every generalizing science the abstract character of the concepts of sociology is responsible for the fact that, compared with actual historical reality, they are relatively lacking in fullness of concrete content' (p. 20).

The Internet is the result, on the one hand, of the US Armed Force's sponsoring of the creation of computer networks for the country's defence at the height of the Cold War, and, on the other, of the libertarian ideals of young university students who, as Padilla (2010) recalls, left their indelible mark on it at the Massachusetts Technological Institute (MIT):

Hacker counter-culture built a wall with passion, addiction, superiority and technical virtuosity that prevented the

<sup>4</sup> Tactics correspond to the weak and his ways of confronting the strongest, in an attempt to have his way, and involve, for example, 'clever tricks, knowing how to get away with things, "hunter's cunning," maneuvers, polymorphic simulations, joyful discoveries, poetic as well as warlike' (Certeau, 1984, p. xix).

military from infiltrating cyberspace. Instead of assuming security, the systems functioned without passwords. Access to computers had to be limited. All the information had to be free. Instead of assuming the military threat, they created art and beauty with computers. Instead of assuming authority, they decentralised it. Under the slogan 'let's get down to it', they infringed the limits. Play and enjoyment were inseparable from innovation and virtuosity. Hackers tattooed that ethic on the DNA of the Internet (p. 75).

## 2. Techno-politics, freedom and war on the Web

The first radical activist groups on the Internet already perceived these contradictions between the freedom offered by the Web and its orientation towards power-related and business purposes, as shown in the early reflection made by the Critical Art Ensemble (1995), one of the most relevant collectives in the 1990s:

Free market capitalism came into conflict with the conservative desire for order. It became apparent that for this new market possibility to reach its full potential, authorities would have to tolerate a degree of chaos. This was necessary to seduce the wealthier classes into using the Net as site of consumption and entertainment, and second, to offer the Net as an alibi for the illusion of social freedom. Although totalizing control of communications was lost, the overall cost of this development to governments and corporations was minimal, and in actuality, the cost was nothing compared to what was gained. Thus was born the most successful repressive apparatus of all time; and yet it was (and still is) successfully represented under the sign of liberation.

However, social movements leveraged ICTs to extend frames of meaning, to innovate their repertoires of action and to enhance their power

and impact at a transnational level. One of the pioneering cases was the Zapatista Army of National Liberation (EZLN), which took up arms in Mexico on I January 1994. The enthusiasm that this rebellion prompted in many parts of the world made sympathisers connect with each other on the Internet to follow the developments in Chiapas and to act in a decentralised manner (Rovira, 2009).

This solidarity network as an additional actor in the conflict worried the Pentagon, which tasked the Rand Corporation, its think tank, with investigating the issue. Ronfeldt and Arquilla (1998) concluded that the Zapatista case was a real netwar—a category that they had already suggested back in 1993—as 'the new form of conflict' in the Information Era. Subsequently, in 2001, these two authors published The Advent of Netwar (revisited), in which they proposed a classification of netwars: those waged by criminal and terrorist groups and those fought by social movements. Ronfeldt and Arquilla boasted that some activists had adopted this terminology, with both the entertainment industry and cinema lending a helping hand. The leftist revolutionary imaginary, based on heroism and sacrifice, resorted to the friend/enemy distinction to understand the political conflicts of the Digital Era. As a framing operation, the 'netwar' lumped together criminal groups, global terrorism and social movements.

Arquilla and Ronfeldt (2001) concluded that a netwar can only be combated with another network. No other avenues, such as extending democratic participation or meeting demands, were considered. Nor would the proposal made by Keck and Sikkink (2000) for thinking in categories such as 'transnational defence networks' take on. For waging counter-netwars, the state's hierarchical organisations would be well-advised to learn from the principles of their adversaries. The Rand's researchers suggested creating hybrid control organisations for mobilising networks with a view to disrupting, contaminating and destroying others. The risks of not doing this properly, in the opinion of Arquilla and Ronfeldt (2001), are high. In this type of conflict, the non-state and transnational actors have had a head start. The problem,

<sup>5</sup> They set early alarm bells ringing about 'potential adversaries, including the non-state sort, who can invent information concepts that may be unusually difficult to combat. This can be particularly the case with psychological aspects and war cultures' (2001).

they note, is that 'network designs imply that militant activism, terrorism and crime are increasingly more amateurish'. Although it is impossible to decapitate a network, they stress that it is indeed possible to slander, to sow suspicion and disinformation, to confuse and to poison the conversation.

The authors recognised a key aspect: according to network logic, information is a 'force modifier'. Mutations, changes in fashion and counterinsurgency can be as simple as flicking a switch: from collective processes that give voice to oppressed groups to hate practices and swinging votes; from citizen journalism to the intentional dissemination of fake news and conspiracy theories. But to flick that switch, money is required above all but not exclusively.

# 3. The means and the ends. Hacker method vs. authority/author/authorised

Versus the instrumental uses of technique at the service of the powers that be, Walter Benjamin (1989) glimpsed a second possibility in his famous passage on the work of art:

The results of the first technology are valid once and for all (it deals with irreparable lapse or sacrificial death, which holds good for eternity). The results of the second are wholly provisional (it operates by means of experiments and endlessly varied test procedures). The origin the second technology lies at the point where, by an unconscious ruse, human beings first began to distance themselves from nature. It lies, in other words, in play (p. 26).

A term deriving from the Web and computational code, the hacker ethic connects with the do-it-yourself (DIY) spirit inherent to punk counterculture; it has a recreational relationship with machines based on a tactical

<sup>6 &#</sup>x27;Yet the more important point is that information, along with the attendant rise of the network form, is a "force modifier".'

act. The field of hactivism, resulting from the union between hacking and activism, has modified the scope of political intervention extending it to the new powers and synergies of cyberspace. Hacking as a method that does not need experts or authorisation, but that learns from anyone and places the accent on amateur enjoyment. Loving more what one does than its results relates to the idea of play and points to an ethic differing from that of capitalism: the hacker ethic (Himanen, 2001).

While self-determining techno-politics is an efficient form of planning, hacking is experimentation. In this sense, the figure of the hacker contrasts with that of the engineer:

To understand how the apparatuses surrounding us work involves an increase in immediate potential, allowing us to act on that which, as a result, does not now seem to us an environment, but a world negotiated in a certain way and in which we can intervene. That is how the hacker views the world (Comité Invisible, 2015, p. 137).

Richard Sennett (2008) includes hackers in his reflections on the pragmatism of the artisan, remarking that his greatest challenge is '[...] to make our particular knowledge transparent in order that the rest should understand and react to it' (p. 355). On the Internet, it is currently possible to find step-by-step instructions and tutorials for making anything, from a souffié to an electronic circuit. Lizama (2005) summarises this hacker ethos and its aspirations: 'Versus the captive user, the self-managed community, versus the inaccessible oligopoly, DIY culture,' versus marketing, the creative reinvention of communication.'

This counter-culture reached a number of milestones, one of the most important being the global movement for free software, founded by Richard Stallman in 1984 with the Free Software Foundation (Stallman, 2010). Padilla (2010) lists others:

In 1990, Mitch Kapor, John Gilmore and John Perry Barlow founded the Electronic Frontier Foundation to defend the

hackers arrested during the first police raid on the computer underground. In 1985, with her A Cyborg Manifesto, the feminist Donna Haraway decried the informatics of domination and celebrated techno-liberation. In 1990, the first hackmeeting was held in Florence (p. 76).

# 4. The advent of hacktivism and the conquest of cyberspace

It was not until the 1990s that hacktivism for emancipatory technopolitics came into its own. The aim of many of the first experiences was to defend the indigenous Zapatista rebels. The art collective Electronic Disturbance Theater (EDT) proposed the idea of electronic civil disobedience and launched a triple attack against the websites of the Presidency of Mexico, the Frankfurt Stock Exchange and the Pentagon, in order to highlight international support for the Zapatists. As a result, 20 million people from all over the world connected to the navigator FloodNet.

However, this soon generated a debate on the ethics of actions of this sort. The proponents of free communication warned about the risks of attacking and manipulating these sites. In defence of the idea of electronic civil disobedience proposed by Critical Art Ensemble (1995) and, subsequently, by Anonymous, it was contended that automated attacks should be avoided, because as long as real people participated in virtual sit-ins or blockades of powerful institutions (never specific people), the political legitimacy of actions of this type was guaranteed.

The yearning for a free, self-regulating Web that was not subject to any kind of laws could be perceived in many allegations and manifestos, including Perry Barlow's 'A Declaration of the Independence of Cyberspace' (1996):

We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different. Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. [...] We must

declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts. We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.<sup>8</sup>

With time, the basic principle of the freedom and self-regulation of the Internet was no longer sustainable. The proliferation of all types of interests that manipulate the conversation has shown that the neutrality of the Web should be guaranteed and that cyberspace is not a liberated territory. On top of all the threats there is corporate interference: the privatisation of the Web 2.0, which profits from user data that has become the new black gold, knows no bounds when inventing services, speeds and terms of use. Moreover, the pay-for-click formula promotes the digital equivalent of junk TV inherent to the mass media age and destroys the compact of intelligibility in the interaction.

# 5. The splendour of emancipatory techno-politics: connected multitudes

To do things with code, with machines, with words, with connections, with interventions, with bodies that gather on the streets. At the turn of the century, contentious collective action became 'connective action' (Bennet & Segerberg, 2012), more prefigurative than programmatic. Smartphones have extended the Internet of the cybercafé or the desktop computer to the streets. The network logic has radically transformed political communication, not only at election time but, first and foremost, for social mobilisation. Connected multitudes (Toret, 2013; Rovira, 2017) convene themselves on online networks and then swarm onto the streets, in a cycle that began with the Arab Spring (Castells, 2012). In Tunisia, at the beginning of 2011, the mass protests triggered

<sup>8</sup> This declaration was presented in Davos, Switzerland, on 8 February 1996, in response to the passing of the Telecommunications Act in the United States.

by Mohamed Bouazizi's self-immolation managed to oust President Ben Ali in only 10 days and sparked similar protests in Egypt and the rest of the countries of the Maghreb. In May that same year, the 15-M movement appeared in Spain and in September the Occupy Wall Street movement surfaced in over 100 cities in the United States. The following year, the Sayonara Genpatsu anti-nuclear rally was held in Japan, while in Turkey in 2013 the protesters occupied Gezi Park in Istanbul. In Brazil, the demonstrations taking place in June 2013 plunged the country into turmoil. This was followed by the Sunfiower Movement in Taiwan and, in 2014, Occupy Central paralysed Hong Kong. In 2016, the #Nuit Debout movement set up its protest camp in Paris, while at the end of 2018, the gilets jaunes blocked the roundabouts of the country's roads and staged protests in cities all over France every Saturday. In June 2019, the masses ousted the governor of Puerto Rico twice. These are only a few examples, among many others, that demonstrate that the most significant changes in the protest movements surfacing all over the world during the past decade are related to ICTs and to political practices that are implemented simultaneously online and in situ: 'on life', which has outpaced the practices of the most traditional leftist social movements and organisations as regards three main aspects:

- 1. The collaborative 'frames of meaning' of collective action (Hunt, Snow, & Benford, 1994), open to the intervention of anyone. The narrative of diagnosis, prognosis and motivation is not controlled by a pioneering group or a leader. Nor do the mass media, not even television, have the last word on defining what is going on. The complexity of the new communication ecology involves a performative constellation of voices, bodies and media, with unexpected results. As noted by Blanco (2014), protest myths have changed: 'Prometheus has taken second place to Hermes, a much more playful and transvestite god, the god of communication and memes, displacing the heroic discourse or legitimisation through sacrifice.' The customs of 'phallogocentrism'
- 9 Blanco defends this hypothesis: 'While the most libertarian May 1968 faced the challenge of sharing metaphors with the tradition from which it wanted to free itself (the Promethean revolution), the 15-M movement has based its objectives, actions and discourses on an imaginary of its time, which has mushroomed in the twenty-first century thanks to the proliferation of the Internet and mobile devices (the Hermesian transformation)' (2014, p. 15).

are being challenged: the prerogative of the white male in all spheres of the construction of meaning, the predominance of leaders and structured militancy. The personal sphere is now considered to be political and there is a growing feminist and hacker sensitivity in the field of action (Rovira, 2018) vindicating 'the commons' as something to be invented and defended against the violent onslaught of the capitalist system.

- 2. The 'repertoires of collective action' (Tilly, 1978) diversify, actions become local and transnational, acting and communicating intertwine, synchronised and decentralised, cybernetic or physical forms are invented collectively or individually. From the most limited forms of participation like clicktivism (or slacktivism) on platforms like Avaaz and Change, to graphics, performances, experiential narratives, confrontation or occupying squares. Connected multitudes manage to orientate themselves on their own and are laboratories in which bodies and symbolic intervention in multiple forms and on multiple scales meet. Actions are self-convened as campaigns that go viral and diversify. The remix, the local adaptation of repertoires and emblems that have been successful in remote contexts, the repeatability of practices and the appropriation of ways of doing things coexist with bodies and their experiences because they are together.
- 3. The 'connective structures' (Martí i Puig & Rovira, 2017) of mobilisations are networks, which implies an approach that is not based on stable structures and which 'opens the code' of protests, highlighting collaboration, replicability, meritocracy understood as a contribution to the community and scalability (Monterde, Rodríguez, & Peña López, 2013). Networks have diminished the difference between the mobilised endogroup and the exogroup or audience; the autonomy of nodes permits intermittency and heterogeneity. Alliances are forged that are neither based on identity-related conditions nor generate unitary processes. According to Barandiaran and Aguilera (2015,

<sup>10</sup> The term 'phallogocentrism' is an neologism coined by Derrida. For a more recent discussion, see Gil (2011).

p. 175), connected multitudes grow without imploding and without a central command as scale-free networks characterised by their robustness (their ability to maintain their essential roles despite perturbations), fiexibility (their capacity to change and adapt to variable conditions) and adaptability (their power to modify their structures and behaviour).

Emancipatory techno-politics appears in the cycle of connected multitudes under the guise of the hacker, as noted by Monterde (2011) when referring to the 15-M movement in Spain:

For those of us who come from the free software age, this mobilisation continually becomes open code. All the content is open data: manifestos, statements, functions. All decision-making spaces are open in the squares, and in forums, and on Facebook, and on pads, and on websites, and on blogs, and in the huge amount of tools invented nowadays. [...] The code of organisational processes is also being continuously copied from one square to another, adapting to the unique needs of each place, working in permanent collective review and modifying its parts to create new prototypes for each one of the realities (p. 1).

In many places, the activists of connected multitudes learn to be 'community managers', to understand how the algorithms of different digital apps work, in order to create trending topics on Twitter and to place issues on the public agenda. In July 2015, a Telegram group in Barcelona posted the hashtag #ThisIsACoup to denounce Greece's third bailout by the European Central Bank (ECB), which subsequently became a global trending topic. Together with 'RIP Democracy', 'Democracy is dead' and the mask of 'Anonymous', there was an avalanche of messages about the financial terms and conditions imposed on Greece, including 'this is a coup', with several media outlets like the New York Times covering the issue.

In Mexico, in 2014, the activists baptised two years before in the connected multitude of #YoSoy132 posted the hashtag #FueElEstado to

express their indignation at the forced disappearance of 43 undergraduates from the Escuela Normal Rural Raúl Isidro Burgo in Ayotzinapa. This protest combined the painting of giant letters in the Plaza de la Constitución of Mexico City with the online dissemination of a picture taken by a drone. A few days later, the Attorney General of Mexico offered a statement in which he claimed that the students had been incinerated in a nearby rubbish dump, a version that did not convince anybody. Faced by repeated questions from the press, the Attorney General said, 'I'm tired of this.' A few minutes later, a video of the press conference entitled, 'Murillo Karam says, "I'm tired of looking for the teacher trainers from Ayotzinapa"', was posted on Anonymous México's Twitter account. In three hours, #Yamecansé had become a global trending topic and continued to be during November 2014, even more so than #Ferguson.

However, after receiving over 4 million mentions, the hashtag was the target of a massive bot attack. According to the network expert Alberto Escorcia, to attack a hashtag as powerful as #YaMeCanse requires the involvement of 50 million fictitious accounts: 'Who has the capacity to hire the thousands of people required to eliminate a trending topic like that?' (Pérez Botero, 2014). The attack consisted in making the hashtag look like spam so that Twitter would eliminate it.

On 31 August 2018, Ludmilla Teixeira, a 36-year-old Brazilian feminist, created a Facebook group called 'All women united against Bolsonaro'. In 48 hours, 6,000 had joined and, three weeks later, their number had risen to 2.5 million (Brum, 2018). The hashtag #ElleNao went viral until reaching the 4-million mark on Twitter. A connected multitude of women took to the streets in Sao Paolo and in other Brazilian cities on 29 September 2018, in an appropriation and remix of the multitudinous Women's March organised in Washington in January 2017 in protest against Trump's recent election.

<sup>11</sup> An action carried out by the Rexiste collective during the mass march on 22 October 2014.

<sup>12</sup> In Spanish, 'Murillo Karam dice - Ya me cansé de buscar a los 43 normalistas de Ayotzinapa.'

<sup>13</sup> On 24 November 2014, the policeman who had shot Michael Brown dead in Ferguson, Missouri, was declared innocent by a jury. In the following weeks, a wave of protests under the hashtag #Ferguson rocked the United States.

Coactive techno-politics was prepared to act in Brazil. The administrators' accounts suffered a massive attack. Flavio Bolsonaro, the presidential candidate's son, in charge of a bot farm (automated accounts), tampered with the same hashtag to disclose the oppression suffered by men.

Determining techno-politics was so intense during Bolosonaro's campaign that, a posteriori, the Brazilian Superior Electoral Court deemed it unlawful to pay online marketing agencies like Quickmobile, Yacows, Croc Services and SMS Market. As Avendaño (2018) explains, 'Firms that offer what is known in the sector as "mass targeting": sending the same message countless times using different numbers (WhatsApp limits the number of times that the same number can send the same text).' The newspaper El País infiltrated one of the WhatsApp groups and received over 1,000 messages a day, the vast majority containing fake news.<sup>14</sup>

How is it possible to hold someone accountable for this? There is no way of investigating these campaigns because only the target accounts receive the messages. In the case of Facebook, not even those who detected political propaganda in their timelines could recuperate it. Mark Zuckerberg, the social networking site's CEO, reluctantly agreed to testify before the US Congress over the scandal involving Cambridge Analytica, an agency that simply closed down so as to avoid being held accountable.

In 2019, the months-long mass protests in Hong Kong received cybernetic attacks promoted by the Chinese government. Twitter eliminated 936 accounts that were being used to 'sow political discord in Hong Kong'. For its part, Facebook only closed 'seven pages, three groups and five accounts', according to Lee (2019).

The netwar, fuelled by a techno-politics at the service of the powers that be and the highest bidder, is here to stay. There is no international legislation regulating the major technological companies or the money that unscrupulously ignores the dividing line between legal and illegal practices, determined to win elections even at the cost of undermining democracies.

<sup>14</sup> For a broad repertoire of these memes, see the report appearing in the El País on 6 May 2019, 'Los Whatsapps de una campaña envenenada'. Retrieved from https://elpais.com/especiales/2018/elecciones-brasil/conversaciones-whatsapp/

Nor is there any way of controlling what states do, even though this signifies interfering in the sovereignty of other countries, as Russia is wont to do.

# 6. Determining techno-politics: terrorism and the ultra-right

According to Weimann (2010), the Internet has enabled terrorist organisations to plan and coordinate attacks, to increase the global reach of their propaganda, to recruit supporters, to communicate with international sympathisers and migrants, to request donations and to enhance their public visibility. Chat forums serve to communicate with sympathisers all over the world and to recruit them with little risk of being identified. This author explains that there are 'experts' directly answering questions about how to mix poison for chemical attacks or how to prepare a suicide attack. Comprehensive instruction manuals have appeared on Paltalk. Furthermore, the cyber-jihad has gone on the offensive: instead of waiting for the unwary to come across their pages, terrorists seek out individuals on their own social networking sites—the same modus operandi employed by pederasts—and design strategies for particular social groups. As Weimann (2010, p. 53) remarks, 'A person in the United States can literally take a terrorist training course within the privacy of their bedroom' (2010, p. 53). Islamists recommend not using Facebook, because it exposes a group of likeminded people as a whole. Al Qaeda's networks promoted its brand by posting videos on YouTube, many of them extremely violent, offering the image of a hydra with a thousand heads capable of acting in different places in the world. It would seem to be the free appropriation of an idea in digital dispersion and a series of values that different nodes autonomously decide to assume and enhance. But that is not necessarily so. The huge amount of propaganda inspired by Al Qaeda is a controlled machine even though it has shifted from private forums or restricted pages towards a much more efficient form of dissemination based on open platforms on the Web 2.0. The research conducted by Klausen, Barbieri, Reichlin-Melnick and Zelin (2012) shows, on the basis of network visualisations, that behind the apparent proliferation of nodes and sources, the main European YouTube channels primarily disseminating

Islamic fundamentalism are associated with the British organisation al-Muhajiroun and work together to spread propaganda and violent content. These researchers analyse how these groups create the best conditions for attracting followers and resort to domain names registered in the United States in order to avail themselves of the First Amendment and circumvent European laws against inciting violence. In other words, Islamic extremism also leverages the level playing field to 'hack' them to its best advantage.

Nor has the far right been slow to spread its tentacles to online communities, with a great deal of success thanks to enormous amounts of money. Its strategies involve disguising itself in trending topics on Twitter or in the algorithms of YouTube to alter them for its own purposes. Lewis (2018) analyses a network of 65 far-right political influencers<sup>15</sup> distributed in 81 content channels on the Internet, including successful YouTubers, scholars, comedians and experts, forming the so-called 'Alternative Influence Network' (AIN), a fully operational media system dedicated to attacking any left-wing position. They manipulate hashtags and on their channels encourage each other to berate feminism, anti-racism or environmentalism, taking advantage of the freshness of network jargon, memes and remixes and employing market research to insert keywords in search engines.<sup>16</sup> YouTube's algorithm, designed to encourage people to remain on the platform and, therefore, to expose them to its ads, tends to drive users to increasingly more violent content.<sup>17</sup> This allows for a broader dissemination of sensationalist news and

- 15 Being an 'influencer' implies creating a personal brand to attract followers on the Internet and to make money from advertising. This new form of communication, art and business combines the glamour of the celebrity world with personal life stories, a powerful formula for conveying gender and race prejudices.
- 16 Marketing companies implement search engine optimisation (SEO) to exploit 'data vacuums' with an eye to 'concealing' certain problems and to sending specific messages to potential target audiences. For instance, some of the videos posted by conservative influencers use the terms 'social justice' and 'leftist' or words such as 'intersectionality' in their titles, in order to appear in search results pages when someone shows interest in such topics.
- 17 This refers to 'the three degrees of Alex Jones': it does matter on which page you start on YouTube, the video of the ultra-right conspirator who contends that the Sandy Hook Elementary School shooting in the United States in 2012 never happened, but that the parents of the victims were actors against firearms, appears in not more than three recommendations.

conspiracy theories. For Tufekci (2018), 'As we click and click, we are carried along by the exciting sensation of uncovering more secrets and deeper truths. YouTube leads viewers down a rabbit hole of extremism, while Google racks up the ad sales.'

One of this ultra-right communication system's celebrities is Steve Bannon, tasked with running the digital propaganda machine for the leave camp in the Brexit referendum in the United Kingdom and responsible for Donald Trump's social media campaign. He also supported Jair Bosonaro's presidential candidacy in the 2018 Brazilian elections.

Steve Bannon relaunched the digital news outlet Breitbart News Network (specialising in conspiracy theories and climate change denial), with the financial backing of the ultraconservative multimillionaire Robert Mercer who, moreover, was the main shareholder of Cambridge Analytica, the political marketing agency belonging to the British consortium Strategic Communication Laboratories (SCL Group), whose mission has been to provide governments and military organisations all over the world with data, analysis and strategies.<sup>18</sup>

In turn, the ultra-right has been developing a broad online community called QAnon, which was launched on the chat channel 4chan (it is no coincidence that it is the same channel from which Anonymous emerged), which is disseminated via encrypted apps like Discord and Telegram. According to Ebner (2019), QAnon has the surprising ability to

link the MI6, Facebook and the Rothschilds to the Vatican, Hollywood, the Nazis, the Illuminati and aliens in order to explain that climate change is a hoax, the Holocaust never happened, the world is run by paedophiles, Satanists and cannibals and that the Queen is a direct descendent of prophet Mohammed.

For determining techno-politics, having a clear-cut objective, being unscrupulous and investing enough money are the keys to success. To these

<sup>18</sup> Marta Peirano reports that the following can be read on its website: 'During 25 years, we have run behavioural modification programmes in over 60 countries' (2018).

Ebner (2019) adds introducing conspiracy narratives in movements to skew existing opposing networks and combining the hashtags of the viral campaigns and trending topics of social activism to alter their political orientation.

## 7. The feminist wave and violent regression

As a result of the global feminist wave, emancipatory techno-politics has spread in the past few years. Since 2015, women have taken to the streets in their masses. The networks of the Web 2.0 and their ability to produce and connect individual stories have favoured a greater feminist sensibility in politics that is embodied in the many accounts of the violence suffered by women from different places and walks of life. Thelandersson (2014) notes,

The Internet provides a space where feminists can learn from each other about why things some feminists see as harmless can be hurtful and offensive to others. Most feminists know about intersectionality, but far from all of us know every way in which intersectional oppression works (p. 529).

Protests and demonstrations are self-convened in multiple spaces on digital networks without the need for formal groups and, in this sense, have opened up feminism to new forms (Baer, 2016). Memes and hashtagbased campaigns, expressions of indignation, the intervention of anyone and its viralisation, have managed to give rise to performative constellations with unprecedented political power that have invaded the streets.

From the Slut Walk to the advent of Femen and Pussy Riot (Rovira, 2018), women's struggles have gone from strength to strength, and not only for combating femicides, with mass demonstrations in India and Latin America with the #NiUnaMenos. Women have also made progress in their struggle for

<sup>19</sup> A term coined by the racism researcher Kimberlé Williams Crenshaw in 1989, which shows that race, class, sex and sexual orientation, among other social categories, are not natural but are constructed in an interrelated way.

equal wages, a cause that reached its major milestone in Iceland in 2016,<sup>20</sup> and against criminalising abortion, from Poland whose draconian abortion law sparked the so-called 'Black Monday' rallies with striking women occupying the streets of 143 cities, to the global wave of green scarves. The women's strike became the protest repertoire of 8 March 2017 and 2018, especially in Spain and Italy.

On the other hand, after the complaints lodged by actresses against the sexual aggressions of the US producer Harvey Weinstein, the hashtag #MeToo<sup>21</sup> was tweeted half a million times on 16 October 2017 and retweeted by 4.7 million people during the first 24 hours (Sini, 2017), until reaching 85 countries, giving rise to many variants and contexts. But all with a common denominator: the aggressive way in which the women participating were treated. Of the 80 women supporting the #MeToo movement in different countries who were interviewed by Mendes, Ringrose and Keller (2018), 60 said that they had immediately been the target of trolls, cyberbullying, harassment and threats. Versus #YoTeCreo that appeared in support of accusations levelled by the members of #MeToo, coactive techno-politics soon reared its head in the form of #YoTeCallo, attacking and silencing them.

As Radsch and Khamis (2013) have revealed in their study, 'In Their Own Voice: Technologically mediated empowerment and transformation among young Arab women', women have been very active in digital networks at a global level and, since the Arab Spring, have created their own cyberactivist culture. Examples include the Riot Grrrl zines movement and the websites of the Iranian feminist movement, in addition to the appearance of female bloggers with a high impact, such as the Tunisian Lina Ben Mhenni, who was 27 in 2011. However, the reaction against them has been one of unprecedented violence until now (Díaz & González, 2016). Amnesty International has reported the persecution, imprisonment and murder of

<sup>20</sup> In Reykjavik, on 24 October 2016, thousands of demonstrators called for equal wages, coinciding with the anniversary of the Icelandic women's strike in 1975. The law guaranteeing this was enacted in January 2018.

<sup>21</sup> The phrase 'Me Too' was first used on Myspace in 2006 to call attention to the sexual abuse of African American women, after Tarana Burke, a 13-year-old girl, had told a community worker that she had been abused.

male and female activists and communicators in all the countries affected by the Arab Spring.<sup>22</sup> It is an unceasing war.

### 8. The state and the netwar

To stay connected people are turning increasingly more to mobile telephones, at the expense of computers—above all the younger generations and in poor countries. Therefore, the information that they access is that provided by apps. Tufekci (2018) analyses how the reception of news is not now individual or attentive, like reading a newspaper, but collective and vociferous, as if we were at a football match: what counts is not the truth but our team. The 'filter bubble of affinity' (Pariser, 2017) promoted by the algorithms of digital platforms reinforces prejudices and whips up hate. While states combine disinformation and propaganda, ordinary people take revenge on each other by posting videos, memes and hate speeches.

In War in 140 characters, Patrikarakos (2017) explains that networks are both centripetal and centrifugal; i.e. just as they can enable people to unite to oust Mubarak in Egypt, so too can they fan the fiames of sectarian conflicts in ways never seen before, dividing Copts, Salafists and the Muslim Brotherhood. The participation of anyone in conflicts via digital networks can lead to both their escalation and polarisation. During the Gaza War, 10 years ago, both sides watched the news on CNN; nowadays they resort to social media.

The Intifada 2.0 got underway in 2015 with images of the mangled corpse of a 21-year-old man killed by a bomb, posted on Facebook by a 19-year-old man accompanied by the hashtag 'The third Intifada has started', which soon went viral. A few days later, he broadcast live his knife attack on two Israelis, before being shot dead. Many decided to follow his example (Le Point, 2015). The State of Israel reported Facebook and initiated high-level talks with Google and Twitter. Thousands of young people have been detained pending trial.

<sup>22</sup> In Amnesty International's report (2016), a young man declares, 'The only gains we achieved during the revolution were our individual and collective freedom. This freedom is now being destroyed in the name of terrorism.'

States are tackling the new conflicts. Bradshaw and Howard (2017) document organisations created in 28 countries whose purpose is to define, monitor and manipulate public opinion on the Web. In 2015,

the British Army announced that its 77th Brigade would 'focus on non-lethal psychological operations using social networks like Facebook and Twitter to fight enemies by gaining control of the narrative in the information age' (Solon, 2015). The primary task of this unit is to shape public behavior through the use of 'dynamic narratives' to combat the political propaganda disseminated by terrorist organizations (p. 4).

Who decides what is a threat and how? In 2013, the Mexican government purchased the FinFisher spyware, exclusively designed for states to help them to combat terrorism and crime. But it used it to monitor the activity of journalists and human rights activists.

Bradshaw and Howard (2017) reveal that 'cyber troops' are actually military units under the aegis of governments, but there are many strategic communication companies that sell their services and sign contracts with the public and private sectors, regardless of whether the aim is to advertise products and services or to engage the citizenry and win their votes. Electoral processes are oiling this mechanism increasingly more,<sup>23</sup> to the point of perfecting new techniques to intervene in all types of networks, as occurred with WhatsApp in the 2018 Brazilian elections, which was inundated with fake news.

Who is responsible for this state of affairs? Who should be held accountable? Governments? Apps? The major digital corporations legislate at a global level with a click through their 'terms of use'. After three years at The Observer working as an investigative reporter, Carole Cadwalladr (2019) accused the 'gods' of Silicon Valley—Mark Zuckerberg, Sheryl Sandberg, Larry

<sup>23</sup> It is evident that political marketing can no longer ignore social networking sites. 'Hashtags—their creation, management and monitoring—have become an element central to any political project or social cause. And a powerful magnet for identifying and measuring behaviours, communities and interests, which allows for the mass management of electoral segmentation and political planning' (Gutiérrez Rubí, 2018).

Page, Sergey Brin and Jack Dorsey (the creators of Facebook and Google and the co-founder of Twitter, who were all in the room during her TED Talk)—of destroying global democracy. She declared that they were guilty of facilitating multiple crimes, before challenging them:

But if they're not sick to their stomach about what has happened in Myanmar or overwhelmed by guilt about how their platforms were used by Russian intelligence to subvert their own country's democracy, or sickened by their own role in what happened in New Zealand, they're not fit to hold these jobs or wield this unimaginable power.

In the Xnet report, 'Acción estratégica y legislativa sobre Fake News y desinformación [Strategic and legal action on fake news and disinformation]', Levi and Guixaró (2019) stress the urgent need to 'create a legal framework that dismantles the disinformation business, in order to put an end to the impunity of major producers and disseminators of fake news and disinformation (governments, political parties, the mass media and corporations)'. Another essential step is to 'pursue the hygiene of the information ecosystem through the transparency and open and distributed verification that many online communities have already put into practice' (Levi & Guixaró, 2019). Fake news is harmful when it is spread on a massive scale and that happens when there are vested interests involved.

# 9. Digital colonialism and technological dependence

In the origins of modernity, Echeverría (2005) explained, 'from being a tool of abundance, the technical revolution has become, in the hands of capitalism, a generator of shortages' (p. 59). For this author, there is a 'systemic trend that has gradually altered the initial position in the appropriation of income, taking it from the fields of landlords to the field of the lords of technique' (p. 19). The relative depreciation of natural products and those of the soil, a catastrophe for agriculture on the periphery of the world-system, which is evinced in the environmental crisis, is now confronting

a new type of technological imperialism.

The companies of Silicon Valley deriving from the libertarian dreams of the pioneers of the Internet, are currently the most powerful corporations in the world and are digitally colonising the planet. The GAFAM group—Google, Amazon, Facebook, Apple and Microsoft—are non-neutral companies, typical of a culture and a language, which practice extractivism in data capitalism and 'concentrate the greatest economic, technological and social power on the planet' (Lechón, 2018, p. 23). Facebook has plans to launch its own cryptocurrency, i.e. Libra, while other platforms have asked banks to share financial information so as to be able to issue credit cards (Ruiz, 2018).

In the current stage, financial capitalism is plundering a new commodity that, as elusive as it seems, is never exhausted: data on human activities and sociability. According to Couldry and Mejías (2019), it is the new data colonialism combining 'the predatory extractive practices of historical colonialism with the abstract quantification methods of computing' (p. 80). For her part, Ricaurte (2019) cautions, 'Our digital selves are quantified and our universe of objects and spaces has likewise been transformed into knowledge that fuels capital accumulation and power concentration' (p. 3).

Many initiatives based on self-management and the cooperative format leverage the Web, but the major corporations of the Web 2.0 are eradicating diversity with their lucrative deals. The paradox is described by the American businessman Tom Goodwin (2015) in the following terms: 'Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate.'

Be that as it may, free culture has led to a burgeoning of practices and projects involving more entertaining forms of technique that do not share the values of capitalism. Its collaborative cathedral is Wikipedia, a project in continual expansion and review, unfinished but, nonetheless, better than any other encyclopaedia ever imagined. Anarchist 'hackerspaces', primarily emerging from the free software movement, have become laboratories in which, in the main, the 'entrepreneurship' of the producers transposes the hacker spirit to the field of innovation for creating new business opportunities ....

## 10. Resistance is life: the exploit

How is it possible to organise the resistance to a faceless enemy? Back in 1995, Critical Art Ensemble was already stressing that neither is power to be found in any place nor does it have a body, but is present in information flows, for which reason the aim had to be to interrupt that flow. This gave rise to Anonymous' DDoS attacks, its appearances in swarms from all directions, hostile intermittency that neither has a figurehead nor a line of battle .... But how is rebellion possible when communication networks are materially in the hands of major corporations and military apparatuses?

In the opinion of Coleman (2018),

What has happened with the Internet also happened with radio, which not only had a tremendous impact on the dissemination of progressive and revolutionary ideas, but also was incredibly important in the development of fascism. In more than one sense, we could say that there has been a reactionary counter-revolution in the use of networks and digital tools.

But neither radio was responsible for fascism not digital networks are the current counter-revolution. The media are mediations. Moreover, the Internet is a re-media—the convergence of many media, formats and languages—and, in turn, a pharmakon—medicine or poison depending on its dose and how it is employed. The fact is that technology has an owner: pancapitalism is researched, implemented and deployed (Critical Art Ensemble, 1995, p. 7).

In the 1990s, when social movements sought to possess computers and modems, a defence mechanism for the Web should have been developed from an autonomous and libertarian perspective. In line with Galloway and Tacker (2007), that possibility was invalidated by the melancholic tendency to always look for lost causes in the past (in this case, the hypnotic power of 1968). In the same vein, Brown claims that the Left is 'caught in a structure of melancholic attachment to a certain strain of its own dead past, whose

spirit is ghostly, whose structure of desire is backward looking and punishing' (1999, p. 26).

For his part, Lovink (2002) regrets the 'light' quality of the social struggles at the end of the last century, which replaced the collective construction of ideas with the creation of informal working networks and which helped to empty politics to give prominence to culture and art, refocusing radical thought on tinkering with software and interface design. Both the hegemonic vision of the Information Society and the activist utopia of the libertarian power of cyberspace have been characterised by a persistent transcendentalism, 'as if the spread of ICT would increase development, as if access to the Internet would improve living conditions, as if free software would override capitalism, as if file sharing equals altruism, as if open publishing would promote democracy' (Lovink & Schneider, 2004).

The difficult quest for new forms of existence, beyond living in the binary keys of identity or in digitalism, is a battle for difference, variation and metamorphosis against the technology and monocultures of corporations. For Galloway and Thacker (2007), these struggles should not focus on changing or abandoning technologies, but on discovering their gaps and identifying potential changes. This is what hackers call 'exploits', i.e. software fragments, data fragments or command sequences employed for the purpose of exploiting the vulnerability of a system. Digital networks amplify action: something small can become larger in a very simple way. These exploits alter the ontology of the Web, for which reason any 'failure' in it is a change in its topology (for example, from centralised to distributed).

For instance, leakers are the exploit. In 2013, Edward Snowden, subcontracted by the National Security Agency (NSA), brought to light classified documents and recorded telephone conversations of the programme PRISM. Gleen Greenwald (2014), the journalist who published these leaks in The Guardian, wrote,

By daring to expose the NSA's astonishing surveillance capabilities and its even more astounding ambitions, he has made it clear, with these disclosures, that we stand at a historic crossroads. Will the digital age usher in the individual liberation and political freedoms that the Internet

is uniquely capable of unleashing? Or will it bring about a system of omnipresent monitoring and control, beyond the dreams of even the greatest tyrants of the past? (p. 17).

In 2006, the cypherpunk Julian Assange created a platform for leaks, WikiLeaks, on which he posted the famous video Collateral Murder, in which a number of US soldiers in a helicopter are seen shooting at people, including two reporters working for Reuters, in Bagdad. In July 2010, WikiLeaks released 70,000 confidential reports on US and NATO military operations in Afghanistan to the world's mainstream mass media. In October 2010, it revealed 400,000 secret military reports on the Iraq War. The person leaking all this information was a 22-year-old soldier called Bradley Manning.<sup>24</sup> In November of the same year, WikiLeaks sent 250,000 US diplomatic cables to 120 journalists working for The New York Times, The Guardian, Der Spiegel, El País and Le Monde. The scandal led to the imprisonment of Manning. Amazon, PayPal, Visa and MasterCard closed the accounts of WikiLeaks. The hacktivist network Anonymous came to the platform's defence by attacking the websites of these corporations and by facilitating the unprecedented dissemination of the leaked cables, which fuelled the revolts during the Arab Spring.<sup>25</sup> Several hacktivists were pursued and arrested.

Manning's, Snowden's and Assange's activities have come at a personal cost, which reveals the implacable violence of the powers that be. Assange will not only be accused of several accounts of espionage for which he could be sentenced to 175 years in prison, if and when he is extradited to the United States, but, as his lawyer Juan Branco explained in an interview,

the press repeated the things with which the powers that be identified him: he was accused of rape, of anti-Semitism, of being a Russian agent. But those discourses came from the

<sup>24</sup> Bradley was his name at the time of his arrest. She is now called Chelsea Manning.

<sup>25</sup> As indicated by Padilla (2012, p. 39), WikiLeaks has been designed as an unfinished device, 'whose real meaning will have to be completed by others', which allows for the emergence of intermediate nodes capable of analysing the different cables and selecting what information to make public.

apparatuses of power with the sole aim of delegitimising a political dissident (Febbro, 2019).

After being cloistered for nine years in a room at the Embassy of Ecuador in London, in April 2019 Assange, now in a poor state of health, was transferred to a high-security prison.

In 2016, the Panama Papers, a series of documents belonging to the law firm Mossack Fonseca, were leaked to the German newspaper Süddeutsche Zeitung and the International Consortium of Investigative Journalists (ICIJ). The documents revealed the tax evasion of heads of state and governments, international political leaders, artistes, personalities from the world of finance and sports celebrities. The person responsible for the leaks, under the pseudonym of John Doe (2016), published a manifesto entitled, 'The Revolution Will Be Digitised', where it is explained how law firms like Mossack Fonseca draft and bend laws at a global level to favour the interests of the wealthiest in a practice of 'generalised mass corruption'. In Malta, the journalist Daphne Caruana Galizia, who played a central role in bringing all this to light, was assassinated in a car bomb attack.

The machinations of Cambridge Analytica were discovered thanks to Christopher Wylie, a young computer expert working for the company who revealed how it managed to obtain the data of 87 million Facebook users<sup>26</sup> with the aim of designing psychometric profiles and disseminating propaganda in favour of Donald Trump, a practice that can be regarded as a psychological war strategy (Cadwalladr, 2018).

From within the system, these cases of leaks are the 'exploit', as with human nature itself, capable of free will and of ethically questioning itself at a given moment. Once life becomes computation, and once information becomes power on the Web, then the Web is controlled by protocols, but with an idiosyncrasy: according to Galloway and Thacker (2007), the government in the real time of the Web is also the dynamic government of life per se or

26 Cambridge Analytica gathered the data of 87 million Facebook users. To this end, it used a personality quiz that Cambridge University's Psychometric Centre posted on Facebook and which was completed by more than 6 million people (Peirano, 2018). In turn, Facebook acknowledged that 126 million people had been exposed to the content of the Russian Internet Research Agency (Elola, 2018)

living networks. Resistance must then counter the way in which the protocol infects and shapes life. For which reason resistance is living persistence.

The world's social movements are becoming more and more prefigurative. Unipersonal ideas and leadership are on the wane. The care and reproduction of life, like the spaces in which women have been historically confined, have become the main focus of resistance, in struggles against precariousness, mine exploitations, agribusiness, impunity, in defence of territory and the environment .... And they open up spaces that politicise vulnerability by appealing to interdependence. As claimed by Butler (2006, p. 46), to consider 'our bodies—as a site of desire and physical vulnerability, as a site of a publicity at once assertive and exposed' (2006, p. 20). That is the way of 'making things and ourselves count' (Rovira, 2017), as opposed to the lives that do not count for money. For Preciado (2018), reactivating desire and the collective body involves breaking with the aesthetic of domination that eroticises the difference between power and perpetuity. The connected multitudes of the twenty-first century seduce in the shared experience of opening up a common horizon and place the spotlight on the feminist maxim according to which the personal is the political, versus exacerbated individualism, neoliberal self-production and the brand-person.

## 11. Counter-insurgency and widespread humiliation

The doomsayers are having a field day. Digital activists have been accused of being naïve and techno-optimists. Perhaps they deserve to be called 'naïve' because of the sheer breadth of the global powers that they are confronting. But not for using digital networks in their favour, insofar as possible, always from hybrid communication systems and in a tactical manner. The constant radical criticism of the Internet as a techno-political device for coaction and control has been precisely made from the hacker universe.

Presenting technology as a whole as a monster advancing relentlessly towards us is in the interests of the global powers that be. Technique is now subordinated to capital, whereby it conceals its failures and its implacable advance. It thus attracts investors and moves higher, pretending to be a linear (without divergences), deterministic (it never ceases to move forward)

and progressive (without errors) process. It overrides any scepticism and convinces us that resistance is futile because 'the technique' is always effective (an ideology indoctrinated throughout the historical process called 'modernity'). But the problem is not the technique or the algorithms, but the goals that drive their development. In this connection, Sadowski (2018) claims that the effectivity of artificial intelligence is still very relative and conceals the role of exploited workers who are those tasked with reviewing data and making decisions. There are a lot of services that make users believe that they depend on robots, but have a backroom in which people are working for miserable wages.<sup>27</sup> Sadowski draws a parallel between present-day artificial intelligence and the Mechanical Turk in 1770, the automaton capable of winning at chess. There was a humpbacked dwarf in the box who moved the pieces on the board. Nowadays, finance is the new dwarf: it moves everything, it invades, tears apart and destroys materiality, it accumulates sociability in the form of data and puts it on ice .... There are waves of connected protests against it, which attempt to decry the terrible ecocidal consequences for our planet, as is the case with the so-called 'Extinction Rebellion'28 in 2019.

The very long shadow of the surveillance and power of algorithmic governance is here to stay. But the new subjectivities and cognitive processes to which digital technology has given rise should be analysed from the social world and its material conditions, and not from technology per se, as the criticisms made by Morozov (2015), Rendueles (2013) and even Han (2014) seem at times.

In his essay entitled, Necropolítica (2011), Mbembe analyses the neocolonial logics that blur the line between politics and war, creating the right conditions for a new racism separating those who can live from those who are expendable or hounded to death. People suffer from the disappearance of

<sup>27 &#</sup>x27;App developers for email-based services like personalized ads, price comparisons, and automated travel-itinerary planners use humans to read private emails. A service that converted voicemails into text, SpinVox, was accused of using humans and not machines to transcribe audio. Facebook's much vaunted personal assistant, M, relied on humans—until, that is, it shut down the service this year to focus on other Al projects.' (Sadowski, 2018).

<sup>28</sup> This online mobilisation phenomenon started in 2018 as result of the call to action of 100 scientists as regards climate change and the initiative of the British organisation Rising Up.

their forms of subsistence, plunged into a competitive, violent, agonising freefor-all. Precariousness (economic, social, environmental) reduces isolation and assuages the fear of insignificance. These are the conditions in which any redeeming (namely, undemocratic) project can come to fruition.

For Preciado (2018), we are experiencing a techno-patriarchal counter-reform, based on a necropolitical masculinity in response to the sexual and anticolonial revolution of the last century. The current fascist trend should be interpreted in terms of the humiliation of the abused masses living in precarious conditions. Bifo expresses it in the following terms:

The feeling of humiliation is more dangerous than that of impoverishment. Impoverishment leads to anger, violence, but also to the rational desire to earn something. Humiliation gives rise to the desire for revenge, even the desire to kill each other ... (Berardi, 2019).

Versus the belief that economic growth and technological development are the only solution to all the problems, Walter Benjamin would say that it is essential to pull the emergency break of the locomotive of history. The German philosopher had dreamed that everyone could be authors. And he pondered on the technical reproducibility of art before reaching the zero cost of the copy, having already augured the loss of the aura and having seen in this a power. And notwithstanding the fact that, as the Mexican anarchist engraver Jonathan Tapia quipped, when interviewed by Josué Pérez, 'Benjamin never watched porn in 4K .... He saw no more than photographs.'

Versus the moral fear of 'technology', it is untrue that digital networks have turned us into sociopaths. But what is indeed true is that majorities are increasingly more violent, displaced, impoverished, sick, anaesthetised and isolated. It is untrue that we enjoy constructing a brand-subjectivity. What is indeed true is that we have no choice but to handle our own branding in order to exist in cognitive capitalism. But that does not do away with the need for tactical capacity, the hacker spirit or the other possible worlds that can now be encountered in this one. As Buck-Morss (2014) remarks, it is essential to speak of the 'global crowd' and of its democratic potential to make it exist.

In the words of Garcés (2017).

The posthumous condition is when a death that is not our real death, but a historical death caused by the dominant narrative of our time, occurs .... But what is at the root of the impotence that defines us in such an acritical and obedient manner as agents of our own end? If we are alive, why do we accept a post-mortem scenario? (p. 26).

### 12. Rails over the sea

The Internet has been equipped with rails. We have ceased to surf in open waters to embark on a customised tour<sup>29</sup> of our own recurrences. Activists (or their melancholies) are not to blame for this, but capitalism that continues to gain ground. It is increasingly difficult to transform the Web owing to the fact that the Internet is not in the world, but is from this world, in a more accelerated, complex, amplified and extreme fashion. A more free Internet will only be possible by constructing a more free society, namely, if we take the reins of the commons and if political democracy triumphs over corporate and financial plutocracy. Fuchs (2011) has no hesitation in claiming that the Internet is both a social medium and a space for accumulation. The corporate fencing in of the commons inherent to the Web 2.0 is a powerful extractivist force, while the political power that serves as a counter-weight does not materialise on its own, but requires prolonged and arduous struggles. The ideology of the Web 2.0 conceals the difference between those two poles, which of course are not equally distributed.

According to Schultz (2018), to flirt with the idea of a mass exodus from Facebook is a hipster illusion, because it does not make anyone less vulnerable or more free. There is no safe zone, for even alternative platforms involve risks. Several studies have shown that even after being erased, any

<sup>29</sup> Tim Berners-Lee resorts to a metaphor: 'Before, we operated on the streets, the world was ours, we entered and left buildings. Now we are enclosed in a shopping centre with strict rules that solely seek to maximise the business model' (2014).

profile can be reconstructed from its environment. We are all in this world. On the streets of Santiago de Chile, on 8 March 2019, there was a placard that read, 'Friend, don't go'. And it was referring to abandoning social networking sites. Who may be interested in silencing the critics? Is abandoning the battlefield a solution?

The Manifesto on Xenofeminism proposes recuperating that hacker spirit in technology to redesign the world from radical diversity. In no uncertain terms, it declares the following: 'Serious risks are built into these tools; they are prone to imbalance, abuse, and exploitation of the weak. Rather than pretending to risk nothing, XF advocates the necessary assembly of techno-political interfaces responsive to these risks' (Laboria Cuboniks, 2015, para. 0x02).

The creative cycle of emancipatory techno-politics has suffered a counter-insurgency involution, to wit, determining techno-politics, an asymmetrical, sly, faceless netwar, capable of buying everything. As Shaviro (2017) observes, it would seem that 'infringement is now fully incorporated into the logic of political economy' (p. 176). Each emancipatory act apparently broadens the scope of the power system. Advertising and political marketing refiect how the creativity and rebelliousness of anti-establishment and countercultural movements serve to continue to sell or to devise the worst ruses to poison the deliberative public space. Campaigns like Cambridge Analytica's that were launched in Trinidad and Tobago in 2010 to dissuade young blacks from voting, thus securing the victory for the party financing them, are terrifying for they raise doubts even about which social movements are actually genuine and which have been induced for unimaginable purposes.<sup>30</sup>

In 2018, Nike posted a popular video entitled, 'Unstoppable Together', recuperating the radical style and message of the global feminist wave. It is increasingly more difficult to distinguish between an ad and a political intervention. The consequences can be both unexpected and functional: Gillette's video about the new non-violent masculinities triggered an unprecedented reaction on social media from men, who posted videos

<sup>30</sup> In the documentary about Cambridge Analytica called The Great Hack, by Karim Amer and Jehane Noujaim (2019), the dancing, music and symbols of what was an induced movement appear on the streets.

of themselves throwing away its products, for they believed that the ad 'castrated' the male sex (Ramírez. 2019).

Lovink (2018) is of the opinion that, now no longer a novelty, the Internet is showing signs of a midlife crisis. Or, like all of us, the Internet simply forms part of the global casino where the house always wins. So, let us just hope that information production, as the production of meaningful difference, is so beyond measure that the excess will become equal to zero. The big data goldmine will become digital rubbish: system overload. It will be impossible to store it, the refrigeration of the cloud servers will collapse, no longer capable of keeping up with the demand, and the bleeding and broken materiality will be exposed. Then, the time, which has always been present, will come: the possibility of constructing, among many and at many levels, the 'data commons' of a technology for a common world, based on collective decision—making.

## 13. Bibliography

















