Technopolitic: sophistication and new dichotomies. The Governments' response to the activists, raises emerging issues.

Francesca Savoldi, Pedro Ferraz de Abreu

Abstract— In the following paper we observe one of the impacts of the new TICs in the context of the recent riots. In particular, we show a few examples where is possible to realize how Governments are experimenting a process of enabling and sophistication, and how TICs could be considered not only a a medium of democratization, but also a new tools of repression in autocratic contexts. Moreover considering the new cooperation between Internet provider and government agencies, we report new issues which must be studied with the aim to improve the structure of the Internet.

Index Terms— Censure, Cyber activism, Internet regulation, Online propaganda, Social Network Site

1 INTRODUCTION

THIS analysis arises from the concern to understand how technology is affecting the social and political changes that we are experiencing. The new revolutions that happened during the last years (especially the last one), have led many to think of the Internet as a medium of democratization.

Actually, the Information and Communication Technologies (ICTs) are facilitating collective action in ways never thought possible, by providing new channels of communication and lowering the cost of organizing collective action, as well as by presenting many other advantages. This has led many Internet optimist to argue that ICTs gave voices to those who had not the possibility to have a democratizing impact around the world [1].

But new concerns are growing over how ICT are sometimes misused, for example by some governments in the context of the recent revolutions. In the following section I will show how in some cases the 'political machine' went through a process that enabled it gaining a power never seen before. This was mainly due to an increasing power compared to that of the netizen's dimension of power and the more easy control of the infrastructures. We are thus faced with a reversal of the phenomenon: while people discover massively the dynamics of revolution and the potential of ICT for their freedom, the same tools are being used to perform new form of repression.

It is therefore highly important to understand how the technology is utilized in the new world scenario, not only with the aim to reach a “scientific consciousness' of the ICT environment, but also to make the masses aware of new risks and new responsibilities in the global changes and find new solutions.

2 SMART OPPRESSIONS.

2.1 A few examples

According to Reporters Without Borders (RWB) in 2011, 5 netizens journalists were killed and 199 blogger and netizens have been arrested experiencing an increase of 30% compared to previous years [2]. According to the 2012 Press Freedom Barometer, 129 netizens have been imprisoned on charges related to the content of their online postings and 7 netizens and journalist were killed, (number which includes only cases in which RWB has clearly established that the victim was killed because of his/her activities as a journalist) [3]. In 2012 the countries with the most imprisoned bloggers were China (68 prisoners), Iran (20), and Vietnam (18) [4].

A report by CNN [5] claimed that dozens of opposition activists in Syria have found their computers infected with malware that can spy on their every move, in a country where more than 400 people have been reported dead in recent weeks [6]. According to Radwan Ziadeh, Founder and Director of Damascus Center for Human Rights Studies [7] in the case of Syria, demonstrators know that if they are participating in anti-government protests, they are putting their lives at risk, because they can easily be checked up on Facebook.

And likewise in other countries considered by the Human Rights Watch as being dangerous regimes or as being countries with a fragile democracy, activists are identified and punished through new strategies.
But what are these new methods of repression?

2.2 Internet censorship and shutting down

Autocratic regimes consider new medias as a threat and they are applying as a consequence new methods of surveillance. Censorship occurs through several ways, the simplest one is to block access to whole domains, which is done by local Internet service providers (ISPs). The Golden shield in China (the great firewall) instead of blocking access, passively monitors traffic at the physical points where fibre-optic links cross the Chinese border. When it sees a word or page address that it doesn't like, it sends instructions to 'shut down' the connection before the web page can load [8].

Filtering sometimes leads to paradoxes, such as in the case of the 'Ayatollah Ali Khamenei', who was censured by the same system that was supported by him more than by anyone else in the Islamic Republic of Iran. The fatwa that Khamenei pronounced on illegality contained the word 'anti-filtering', which is one of the prohibited expressions that are automatically blocked by the safety system, with the result that the Iranians have not been able to read the judgment [9].

2.3 Controlling infrastructures

In 2011 the Chinese government announced a plan to track the cell phones of the 17 million inhabitants of Beijing, with the aim to improve traffic. The announcement came at a point of heightened awareness of the use of mobile devices and Internet communications sites such as Facebook and Twitter in organizing and fueling civil protests against the governments of Egypt, Tunisia and Libya [10].

After the London riots in August 2011, a statement by U.K. Prime Minister David Cameron planted the idea of increased monitoring of British citizens via their cell phones. London's Metropolitan police department has purchased technology from Datong that is meant to be 'a mobile phone network, transmitting a signal that allows authorities to shut off phones remotely, intercept communications and gather data about thousands of users in a targeted area [11].

On December 2011 in San Francisco hundreds of people turned out at BART stations to protest against the July 3 killing of a man during a confrontation with transit police. The statement released by BART said they asked wireless providers to temporarily interrupt service and select BART stations as one of many tactics to ensure the safety of everyone on the platform. The deputy chief communications officer for BART told that mobile services were disabled in four San Francisco stations from 4pm to 7pm local time. The rail transit provider in the United States disabled mobile phone services to prevent a planned protest [12].

2.4 Controlling infrastructures

According to a inquiry of Bloomberg in 2011 [13], Italian technicians in telecom offices from Damascus to Aleppo have been busy equipping the Syrian President Bashar al-Assad's regime with the devices to intercept, scan and catalog virtually every e-mail that flows through the country. The Italian enterprise Area SpA is installing the system under the direction of Syrian intelligence agents, with which the regime will be able to follow targets on flat-screen workstations that display communications and Web use in near-real time alongside graphics that map citizens networks of electronic contacts, enabling the Assad's government to dip virtually into the Internet in Syria.

In Egypt in 2009 the British company called Gamma Group International offered a monitoring software called Finfisher to the State Security Investigations (SSI), which has the ability to send fake updates for popular software, from Apple, Adobe and others that can infect computers with surveillance software, according to one of the company's marketing videos [14]. The SSI have been described in their internal communications as an “high-level security system that has capabilities not provided in other systems, the most prominent capability being to hack into personal Skype accounts, hacking email accounts associated with Hotmail, Yahoo and Gmail, completely control targeted computers. In another communication in December 2010 they affirmed that SSI can “record audio and video chats, record activity taking place around hacked computers with cameras and take copies of its content' [15].

In Russia on March 2012, a wave of spam e-mails promoting a rally against Putin was delivering the spyware as an attachment that appears to be a Word document. In reality, the file is a software program known as "Trojan.Dropper". Mails, whose subject line said "all for demonstration" or "meeting for fair elections", have a body pushing the recipient to open an attachment, purporting that it contains need-to-know information. Symatec says that the Trojan. Dropper is attempting to connect to a server located in Switzerland, but it is associated to another notorious virus that once operated from a Web address with a Russian domain name. Once inside the computer, the virus overwrites many of the user's files then deletes them thoroughly, causing it to blue-screen [16].

2.5 Online propaganda

According to an inquiry of the Institute of International Relations of Taipei, the Chinese government is managing the online public opinion through digital propaganda. The commentators are employed by the Chinese authorities to influence public opinion online (they are known as the "fifty cents army") by managing online opinion through monitoring. China's cyberspace and blogosphere includes popular discussion forums and blogs, where the "fifty cents army" is posting comments in order to mold public opinion and turn negative or critical opinions into favorable ones. Less than two decades ago Chinese government embraced ICT in order to be more competitive at the international level, but these new tools were also used by the citizens as a space for political discussion, reaching a popularity that couldn't be ignored by the authorities [17].

As is claimed in an article of The Guardian [18], the Russian army of Anonymous hacked thousands of emails of the youth group Nashi (a vast network of bloggers, journalists and internet trolls) and discovered that they had been paid hundreds of thousands of pounds to create flattering coverage of Vladimir Putin and discredit his political rivals. The emails of the Nashi included the price list for leaving hundreds of comments and negative stories about Putin, plans to purchase a series of articles about Nashi's annual Seliger summer camp in two popular Russian newspapers and calls for paid Nashi activists to "dislike" anti-regime videos posted on YouTube.

3 DUALITY IN THE ICT'S ENVIRONMENT

With these cases we can see that the excessive optimism around ICT in politics is groundless, given that governments have now learned the potential of these tools. Repression is becoming more sophisticated, not just in censuring, blocking, monitoring and limiting Internet access and doing propaganda with dirty tricks, but also in a proactive way: throwing cyber-attacks, threats and making propaganda. It has also created Self-defense systems of second degree such as the panic button: an application that in case of the confiscation of their mobiles by the police or government agencies, will wipe the cell phone's address book, history, text messages and broadcast the arrest as an emergency alert to fellow activists.

In the considered cases, the response of the "political machine" to the protesters can demonstrate that technology is instrumental. It is a channel that can be manipulated in different ways: freedom but also new crimes have been born online.

So we can say that the question of whether ICTs foster democracy or surveillance and anti-democratic behavior, makes no more sense. In fact the paradox is another: while the people discover the potential of the Internet for their freedom, it is at the same time becoming a tool of repression not only of politicians, but of a capitalist elite, that accumulates the control of politics and economy. The Internet depends largely on private companies for providing access, connectivity, hosting, and online forums. Moreover repressive governments negotiate with private companies that provide them softwares and services for their sinister tactics. Absurd scenarios are happening: the European Union is imposing sanctions against regimes, banning arms sales, but it doesn't forbid European companies to sell surveillance technology. Are these not weapons in another format?

Seeing the cooperation between private companies and government agencies in this context, it is easy to assume the necessity of a Internet regulatory framework, but who should define it? Governments or private companies? And here comes the first dichotomy: free Internet vs regulated Internet.

UNESCO published 2011 the 'Freedom of Connection Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet' which was a commissioned research that is supposed to suggest to politicians what Internet practices should be taken into consideration. But it is hard to believe that the regimes will consider it.

As a consequence of this argument a second dichotomy arises: surveillance vs. anonymity. If the Internet is not regulated, it is necessary to consider anonymity as a natural mechanism in self protection; in a speech on Jan 2010 Secretary Clinton said anonymity protects the free expression of opposition in front of repressive governments. Anonymity allows the theft of intellectual property, but anonymity also permits people to come together in settings that give them some basis for free expression, without identifying themselves [19].

But to be anonymous, one must be aware of the reality of the network. I would like to evoke here the rhetorical duality described in The net delusion [20] Cyber-utopia vs. cyber-realism. If the cyber-utopian ideology is proving to be naive, the only way not to consider the network as a dystopia is to develop a mass consciousness and to understand the rhythms of change of the network itself.

CONCLUSION

After analyzing some cases of digital repression in the context of the recent riots, which have developed in various ways including Internet censorship, shutting down, control of infrastructures, collecting data, content/cyber attacks and online propaganda, we can say that the sophistication of regimes debilitates the excessive optimism created around the ICTs. We see how technology represents an instrumental tool: it seems to be a channel, which can be manipulated in different ways.

So instead of thinking if the ICT fosters democracy or control, it seems more interesting to shift the focus on a new paradox: while people massively discover the potential of the Internet for freedom, it is also becoming a tool of repression not only for a political class, but for a capitalist elite, given that the Internet depends largely on private companies.

Based on this argument the new dichotomies emerge as: free Internet vs. Internet regulation, surveillance vs. anonymity, cyber-utopia vs. cyber realism. These are topics to be deepened and guidelines, on which to build the new structure of the Internet.

ACKNOWLEDGMENT

This work was supported by a grant from FCT (Fundação Ciência e Tecnologia).

REFERENCES

[1] J. Friedland,K. Rogerson. *Political and Social Movements Form on the Internet and How They Change Over Time.* Institute for homland Security Solution, 2009.

[2] Reporter Without Borders. *The 10 most dangerous places for journalists.* Published on 21 December 2011 on http://en.rsf.org/annualoverview-21-12-2011,41582.html

[3] Reporter Without Borders. *2012 : 22 Journalists killed. Press Freedom Barometer 2012.* Retrieved from http://en.rsf.org/press-freedom-barometer-journalists-killed.html?annee=2012

[4] Y.J. Lim, E.S. Sexton. *Internet as a human right: a practical legal framework to address the unique nature of the medium and to promote development.* Washington Journal of law, technology & arts Volume 7, issue 3 winter 2012.

[5] CNN. *Computer spyware is newest weapon in Syrian conflict.* Published on February 17 2012 on http://articles.cnn.com/2012-02-

17/tech/tech_web_computer-virus-syria_1_opposition-activists-computer-viruses-syrian-town?_s=PM:TECH

[6] Electronic Frontier Foundation. *EFF opposes CISPA on Hackers and founders Panel.* Published on April 20, 2012. https://www.eff.org/deeplinks?page=7

[7] Yalibnan. *Interview with Radwan Ziadeh: "The Syrian revolution is the revolution of YouTube".* Published on yaLIBNAN on July 21 2011. http://www.yalibnan.com/2011/07/21/ziadeh-syrian-revolution-is-%E2%80%9Cthe-revolution-of-youtube%E2%80%9D/

[8] M. Luff for RUSI. *The Green Counter-Revolution: Iran Steps Up Its Digital Offensive.* Royal United Services Institute. Published on rusi.org/analysis/commentary/ref:C4E5F66F731EAB

[9] Businnes Insider International. *Iran's Online Censor 'Filtered' The Ayatollah's Fatwa On Antifiltering.* Published on Businnes Insider International May 9, 2012. http://www.businessinsider.com/irans-online-censor-filtered-the-ayatollahs-fatwa-on-antifiltering-2012-5

[10] The Washington Post. *China plans to track cellphone users, sparking human rights concerns*. Published on March, 3 2011 on The Washington Post. http://voices.washingtonpost.com/posttech/2011/03/china_said_it_may_begin.html

[11] The Guardinan. *Met police using surveillance system to monitor mobile phones.* Published on The Guardian on October 30, 2011. http://www.guardian.co.uk/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance

[12] Aljazeera. *US railway blocked phones to quash protest* . Published on Aljazeera on August 13, 2011. http://www.aljazeera.com/news/americas/2011/08/201181221139693608.html

[13] Bloomberg. *Syria Crackdown Gets Italy Firm? Aid With U.S.-Europe Spy Gear.* Published on Bloomberg on November 3,2011. http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html

[14] The Wall Street Journal. *Surveillance Company Says It Sent Fake iTunes, Flash Updates.* Published on The Wall Street Journal on November 21,2011. http://blogs.wsj.com/digits/2011/11/21/surveillance-company-says-it-sent-fake-itunesflash-updates-documents-show/

[15] Advocacy. *Egypt: how companies help the government spy on activist.* Published on Advocacy on May 7, 2011. http://advocacy.globalvoicesonline.org/2011/05/07/egypt-how-companies-help-the-government-spy-on-activists/

[16] CNN. *Spyware assails Russian opposition members*. Published on CNN on March 9, 2012. http://articles.cnn.com/2012-03-09/tech/tech_web_spyware-russian-opposition_1_mails-antivirus-software-symantec?_s=PM:TECH

[17] Hung Chin-Fu. *China's Propaganda in the Information Age: Internet Commentators and the Weng'an Incident*. Issues & Studies 46, no. 4 (December 2010): 149-180.

[18] The Guardian. *Hacked emails allege Russian youth group Nashi paying bloggers.* Published on The Guardian on February 7, 2012. http://www.guardian.co.uk/world/2012/feb/07/hacked-emails-nashi-putin-bloggers

[19] H. Rodham Clinton. *Remarks on Internet Freedom.* Conference at The Newseum on January 21, 2010. Published on U.S. Department of State website. http://www.state.gov/secretary/rm/2010/01/135519.htm

[20] E. Morozov E. *The net delusion.* Public Affairs ISBNS 978-1-58648-874-1

- *Francesca Savoldi, e-Planning PhD student, researcher at CAPP, UTL-ISCSP, Universidade Técnica de Lisboa. E-mail: fsavoldi@gmail.com*
- *Pedro Ferraz de Abreu, Principal Researcher at CAPP, Head of "Technology, Society and Governance", Invited Full Professor at UTL-ISCSP Universidade Técnica de Lisboa , Research Associate at DUSP-MIT , E-mail: pfa@mit.edu*