Infowar in Syria: The Web between Liberation and Repression

Sofia El Amine
UIR Web Science - CEMAM
Saint-Joseph University
Beirut, Lebanon
Sofia.amine@usj.edu.lb

Stéphane B. Bazan
UIR Web Science - CEMAM
Saint-Joseph University
Beirut, Lebanon
Stefan.bazan@usj.edu.lb

Sabrine Saad
UIR Web Science - CEMAM
Saint-Joseph University
Beirut, Lebanon
Sabrine.saad@usj.edu.lb

Lorraine Etienne
UIR Web Science - CEMAM
Saint-Joseph University
Beirut, Lebanon
Lorraine.etienne@usj.edu.lb

Addis Tesfa
UIR Web Science - CEMAM
Saint-Joseph University
Beirut, Lebanon
Addis.tesfa@usj.edu.lb

Christophe H. Varin
UIR Web Science - CEMAM
Saint-Joseph University
Beirut, Lebanon
Christophe.varin@usj.edu.lb

WebSci 2012, June 22–24, 2012, Evanston, Illinois, USA.
ACM 978-1-4503-1228-8

Abstract
In this ongoing research, we propose an interdisciplinary interpretation on why, in the Syrian context, the Web has not yet brought the expected changes witnessed by other countries touched by the Arab Spring. The fact that the Syrian revolt came just after the revolutions in Tunisia and Egypt gave a decisive advantage to the regime. After 12 years of complete black-out, the repressive system gave free access to social networks and microblogging sites to the public in Syria. This move was intended to take a strategic position on these networks to fight a civil Infowar on the protesters. The Web, in its distributed form, is used for online guerilla by Cyber Activists, but well-organized repressive forces can definitely use it as an effective weapon of *mass-repression*.

Author Keywords
Society; Syria; Revolution; Arab World; Infowar; Cyberwarfare; Civil War; Repression

ACM Classification Keywords
K.4 Computers and Society. K.4.1 Public Policy Issues: *Use/abuse of power*

General Terms
Human Factors

	**Syria**
Population	**22,500,000**
Internet users in 2000	**30,000**
Internet users in 2011	**4,500,500**
Websites closed in Syria until 2011	Facebook Twitter Wikipedia Amazon Blogspot Israeli news sites (All) Lebanese news sites (Some)

Table 1. Sources: ITU, Syriatel.

Introduction

The "Arab spring", as referenced in the media, was made possible by the use of the Web by dissidents, as a tool among others, in the process of structuring and organizing protest. The numerous platforms, software, applications available on the Web, described by journalists and scholars as vectors for democratic change, have not yet had such an effect on the Syrian Crisis scene. So far, the ongoing events have not been qualified by the international media as part of the "Online Social Media revolution" that took place in Tunisia or Egypt. When bloggers in Egypt and Tunisia had a decisive advantage given by their long time experience of digital activism online, the situation is seemingly much more complex in Syria, where "Cyber Activism was born during the protest, in a very difficult context" [De Angelis, personal communication]. The regime, helped by external support, is using the Web as a tool of repression and control. In that perspective, we are trying to underline the Syrian specificities in the use of the Web as a weapon in an Infowar. We raise the following questions: considering the Syrian context, could the Web be used both for liberation and brutal repression? Is it facilitating or on the contrary endangering the revolutionary process? This research reports examples and observations from both aspects and provides a typology of techniques used by belligerents. Our precedent research on the Web as a new battlefield between asymmetric powers during the 2006 war in Lebanon finds here an interesting "reversed" echo.

Infowar and the Syrian context

The first "online civil Infowar"

Infowar on the Web was described in a 2001 report as "battle space digitization, a process that will irremediably and sometimes unpredictably influence the art of command and the use of forces" [1]. Next generation conflicts and the very nature of war will largely be influenced by battle space digitization. Whereas victory used to be dictated by fire, movement and choc, it now consists in "overcoming, thanks to information". What are the characteristics of that new form of warfare called "*Infowar*"?

Information Warfare designates all the methods and actions, using new information and communication technologies, carried on in order to inflict damage to the opponent, or insure one's superiority. In other words, "if information is an instrument of national, global, and corporate power, control over its use, its protection, and its manipulation, are national and global security issues" [2]. Studying Infowar means understanding examples of strategic and tactical offensive and defensive aspects of Information operations (IO) on the Web, by state and non-state actors to achieve political, military, and economic goals through IO means, including psychological operations (PSYOPS), perception management, media manipulation, propaganda, strategic influence, and public diplomacy, among others.

Methodology

This research complies with the requirements of interdisciplinarity and mixed methods of Web Science: quantifying Cyber Activism by identifying all reported traces of Infowar activities and interpreting, with a qualitative political science approach, the strategic dimensions of each move, considering that the Syrian context is definitely original. If the quantification process is difficult for technical reasons (few trusted data sets and a highly dynamic and volatile content –

Fig. 1: The official Al Assad page on Facebook

Fig.2: The Syrian Revolution 2011 page on Facebook

Facebook and YouTube are very prompt at removing pages or content), we followed an iteration process, to produce a detailed typology of actions, means and actors. The research also needs to prevent deception by online activists from both camps and allied parties.

Characteristics of the Syrian Context

The Syrian revolt against the Syrian regime started in late February 2011 and the country is today on the verge of a large scale civil war. During this year of conflict, Information warfare on the Web played an important role in the protest mobilization, but also in the repression organized by the regime. Web sites and social media platforms have been a weapon of choice for both dissidents and forces loyal to the Syrian Regime. This balance can be explained by the fact that, having observed events in Tunisia and Egypt, the Syrian government realized quickly the importance of online mobilization and was able to take a decisive advantage of it in order to track and monitor the Syrian dissidents. The Syrian government, in an unprecedented move, opened access to sites such as Facebook, Twitter and YouTube after having blocked them for 3 years (from 2007 to 2010 – Even if Al Assad had an active Facebook profile at the time [3] – *Fig.1*). The move follows the fall of El-Abedine in Tunisia and Moubarak in Egypt [4]. They obviously learned the lesson. Researchers, like Helmi Noman [5] have stated, almost at the same time, the creation of the "Syrian Electronic Army (SEA)" who supports the Syrian Regime and use Social Media to track and discredit dissidents.

In the context of the Arab Revolts, the Syrian case seems to be slightly distinct. In fact, after the Tunisian and Egyptian experiences, the Syrian Regime acknowledged the significance of social media and the necessity to control it and use it[1]. Furthermore, when Syria's government unblocked access to social networks in February 2011, many of the Cyber Activists saw it like as an opportunity for more freedom of speech. When Egyptians were denied access to Internet connections and mobile 3g, the Syrians could, for the first time, open accounts on Social Networks and blog platforms. Contents were highly polarized: For the first decade of Assad's presidency, most Syrian blogs were fairly supportive of the regime because of its commitment to the Palestinian cause and its opposition to the United States and Israel. With the revolt, many Syrian bloggers (intellectuals, journalists and ordinary citizens) have steadily joined the anti-government camp and a number of them have written compelling mea culpa [6]. In the beginning of the uprising, many of the demonstrators didn't hide their identities and were unmasked. The authorities started requesting Facebook passwords and IDs from the dissidents, and used social networks to collect personal information and control private life [7]. Therefore, social networks gave a real opportunity for the government to track down insurgents. Also, according to De Angelis, "Net Activism is more separated from the protests on the street and net-activists lack coordination. They didn't guide the protest or offer a platform where opposition movements could negotiate a unified political line".

[1] Speech by President Al Assad at Damascus University, 20 June 2011

Online Civil War techniques in Syria

Exfiltration of content for global awareness
In the context of the Syrian Online Civil War, Social Media tools are weapons of choice. If the Web is a free, open and distributed space where collective action can easily be traced, individuals may use it as a place to hide and fight undercover. Despite a lot of technical problems and genuine experimentation, Cyber Activists in Syria succeeded in nurturing a global culture of online activism (even if bloggers communities were officially forbidden). For example, by December 3, 2011, there were 395,000 visual clips on YouTube tagged in English or Arabic as related to events in Syria. In 2011, around 56,700 new videos were uploaded, compared to only one third of this number back in 2010. Many of them were published from inside Syria, although the exact number remains unknown, as Syrians often use software (like VPN) which makes their locations difficult to detect [8]. Syrian bloggers like Hussein Ghrer (ghrer.net/blog/) have become national heroes and played an essential role in the report of news to the outside world by documenting content of events taking place. This was achieved through the most dangerous means: Turkish and Lebanese authorities reported digital video content smuggling activities across the border of Syria[2].

Deception and manipulation
International Websites and social media platforms have relayed Cyber Activists documentation of violence. In such a complex situation, inexperienced usage of online mobilization lead to contents (video and images) sharing without verification. These actions of "publish, then filter" [9] were strongly criticized due to the lack of accountability and the existence of obviously deceptive content in what Innis defines as "communication bias" [10]. The sad example of the "Gay girl of Damascus" speaks for itself [11].

Globalized Infowar
Another aspect of the ongoing mobilization of the online communities is the actions conducted by the group calling itself *Anonymous*, which conducted defacement and DDOS attacks on Syrian official web pages[3]. Anonymous has officially claimed the 8/8/2011 attack against the Syrian ministry of defense website homepage that was replaced with the Anonymous logo and a call for the downfall of the Syrian Regime. The group has gone further and hacked into the personal E-mail of Al Assad and published parts of seized messages. Defacement needs to exploit vulnerabilities that can range from weak passwords, path traversal or vulnerabilities on the servers. DOS or DDOS using tools such as LOIC (Low Orbit Ion Cannon), #RefRef or Slowloris, were used by *Anonymous,* along with Botnets like ZeuS, used to attack Syria's financial system [12].

The Web used for repression
If Syrian Cyber Activists fought the regime through relatively classic means, like Facebook groups and pages (*Fig. 2*), twitter accounts or upload of videos on YouTube, the reaction of the authorities was much more elaborated than in other Arab countries shaken by

[2] Lebanese Armed Forces members unofficially reported that portable hard disks containing video content to be uploaded were seized at the border in November 2011.

[3] Anonymous communications, Anonymous hackers: "Congratulations Mr. Assad, You have received the undivided attention of Anonymous", June 2011

Fig.3: Harvard University website hacked by the SEA (*Source BBC*).

Fig. 4: YouTube page of a Syrian Hackers School Member.

revolts. The Syrian regime is way more organized with a rather efficient and obedient vertical organization while the other side is a more horizontal and networked organization. This leads us to say that the ongoing battle for information on the web is to be categorized as *asymmetric* Infowar, since the parties are not of equal size and act following different organizational capacities. As soon as February 2011, Government hackers launched what Web security experts call "man in the middle" attacks on Facebook users by inserting a false "security certificate" onto people's web browsers when they log into their Facebook accounts through the secure "https" version of the site [13]. These attacks enabled pro-government hackers to take control over Syrian activists' accounts and obtain access to their entire network of contacts [14]. Cyber Activists like Razan Ghazzawi of Global Voices Online were arrested and the Electronic Frontier Foundation lists 12 Cyber Activists still under custody [15]; others were forced to flee out of the country.

The Syrian Electronic Army

In the same time, The Infowar Monitor [16] started recording and documenting the activities of the Syrian Electronic Army (SEA), which appears to be a case of an open and organized pro-government computer attack group that is actively targeting political opposition and Western websites. Their site is hosted by the government-related Syrian Computer Society and they recruit supporters and hackers through their "Syrian Hackers School" (Fig. 4). That report documented how Syria has become the first Arab country to have a public Internet Army hosted on its national networks to openly launch Cyber attacks on its enemies.

The *Syrian Electronic Army,* which depicts itself as an organization of volunteer supporters of the regime, is officially involved in promoting pro-regime information on Web social media such as Facebook, Twitter and YouTube. But they also undertake high profile defacement attacks (122 domains on June 4, 2011) on sites deemed hostile, such as those seen on the Qatari TV Al Jazeera website, BBC News, Harvard University (Fig. 2) or on Israeli Websites [16]. According to the Infowar Monitor report, "many of these defaced sites share IP addresses, indicating that far fewer compromises actually occurred than what appears upon first glance". The SEA created a deceptive YouTube site hosting opposition videos to attack visitors' computers with Trojan viruses. Other techniques include DDOS attacks, URL defacement, "man in the middle" attacks [17] and forged certificates [18] on social media sites. Dos software is available for download on the SEA's Facebook page. SEA is also responsible for monitoring opposition Facebook pages, replace original content and steal users' credentials via the web (or via physical coercion in connection with police forces) in order to monitor these people's activities and contacts. They also use viruses and Trojan to scan computers and Facebook accounts in order to find any data that may implicate them. This is furthermore done to propagate pro-regime information via the compromised accounts of Cyber Activists which reputation as regime opponents has been established. Other reported ways of Infowar include *malware* and *Trojan-type viruses'* dissemination, which collect credentials from opponents.

Conclusion

The situation in Syria is still very complex and what will happen next, on the ground and on the web, is very

difficult to predict. The strategic positioning of belligerents leads to an online civil war, a first case to be observed in history. The regime has a precious advantage, thanks to a structured and efficient repressive organization. The protesters, in a really different scheme from the Tunisian and Egyptian models, struggle to coordinate action and negotiate a strong and unified political opposition. This research project will to collect the highest number of evidences of this exceptional situation and document potential new forms of Infowar on the Web.

References

[1] Soubirou, G. *Report on the battle space digitization*, n°11/33/CDES/CAB, Feb. 2001.

[2] Taipale, K. *Overview of the Program on Information and Warfare*, Global Information Society Project, World Policy Institute. May 2011.

[3] Bazan, S., Varin, C. *Web Science in the context of the Arab Near East.* In: Proceedings of the WebSci10: Extending the Frontiers of Society On-Line, April 26-27th, 2010, Raleigh, NC: US.

[4] Preston, J. *Syria restores access to Facebook and YouTube*. The New York Times. 9 Feb. 2011.

[5] Noman, H. *The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army*, OpenNet Initiative, June 2011.

[6] Muhanna, *E. Syria's defecting bloggers*. IHT Global opinion. Dec. 2011.

[7] Al Chalabi, M. *Civil War in Facebook: Towards Which Syria are we moving to? Al-Akhbar***,** 16 May 2011.

[8] *Data taken from "Syria on the World Wide web"*, Syria Today, Jan. 2012.

[9] Shirky, C. *Here comes everybody. The Power of organizing without organizations*. New York. Penguin Press. 2008.

[10] Innis, H. *The Bias of communication*. Toronto University Press. 1991.

[11] Gonzalez Quijano, Y. *Les spin doctors du Net : la vraie vie de la Gay Girl in Damascus.* Cultures et politiques arabes, June 2011.

[12] Zeus Trojan Invades Syria's Financial Sector. http://www.thenewnewinternet.com/2010/11/16/zeus-trojan-invades-syrias-financial-sector/

[13] Facebook users in Syria targeted by cyber attack. http://www.ameinfo.com/264319.html

[14] Syrian spyware targets opposition. http://thehackernews.com/2012/02/syrian-spyware-to-target-opposition.html

[15] Sutton, M. *Syria Arrests Razan Ghazzawi and Eleven Other Activists in Renewed Crackdown of Online Dissent*, Electronic Frontier Foundation, www.eff.org, 2012.

[16] The Infowar Monitor. *Syrian Electronic Army: Disruptive attacks and hyped targets*. http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/

[17] Liebowitz, M. Syrian Facebook users hit by Online Attacks. In: Security News Daily. May 2011.

[18] Leyden, J. Fake certificate attack targets Facebook users in Syria. The Register. May 2011.