الملخص

حرب المعلومات على الشبكة العنكبوتية في منطقة الشرق الأوسط

سبرين سعد ، ستيفان بازان وآديس تسفا

تُعرَفْ منطقة الشرق الأوسط في العالم كمنطقة النزاعات السياسية والعسكرية، منذ العام 1948. وقد شهدت هذه المنطقة العديد من النزاعات، لكن جديدها يكمن في قدرة السكان المحليين على الوصول إلى شبكة الإنترنت ومعرفة استعمالها. إن زيادة سرعة الشبكة وعدد مستعمليها منذ العام 2005 قد وفَّرَت فرصاً جديدةً للحشد عبر الإنترنت ولحرب المعلومات. فالاستعمال المنظَّم والفعّال لمنصَّات وسائل التواصل الاجتماعي قد غَيَّر المشهد السياسي في العديد من البلدان العربية بين العام 2009 و2011، خصوصا" خلال الفترة المسمّاة "بالربيع العربي". إنَّ محاولة تقييم ما يحدث حالياً في العالم العربي يحتاج أولاً إلى تعريف بشكل واضح مصطلحات حرب المعلومات والحرب الإلكترونية. يوفِّر هذا البحث توطئة للاتجاهات المنهجية الذي يجب اعتمادها لتحديد النشاطات المرتبطة بالشبكة العنكبوتية وقياس أثرها في هذا السياق المحدد. إنَّ الأبحاث المرتبطة بحرب المعلومات على الشبكة العنكبوتية ما زالت في مراحلها الأولى والسعي إلى تحديد ماهية النشاطات المرتبطة بحرب المعلومات على الشبكة يحتاج إلى العمل على المستوى المنهجي والعلمي.

الكلمات المفاتيح: الشبكة العنكبوتية؛ حرب المعلومات؛ الشرق الأوسط؛ الربيع العربي؛ البلدان العربية؛ لاعبون صاعدون.

Introduction

The Middle-East region is known throughout the World for its ongoing political and military conflicts. Since 1948, the region has witnessed many forms of confrontations, but recent ones have found new strategic orientations with the development of Web access and literacy, among local populations. Increase in networks speeds and democratization of Internet connections since 2005 have created new opportunities for online mobilization and information warfare. Organized and efficient usage of Online Social Media platforms has altered the political landscape in many countries of the region, during the 2009 -2011 period now called the "Arab Spring"(1). Even if the "Google Doctrine's", described by Morozov as "the enthusiastic belief in the liberating power of technology accompanied by the irresistible urge to enlist Silicon Valley start-ups in the global fight for freedom"(2)is largely criticized today, it's an establishedfact that Web platforms and tools, used by citizens or governments, have created new virtual zones of conflict. To evaluate what is really going on in these new zones requires a clarification of several misunderstandings in definitions of information warfare and cyberwarfare.

This paper offers methodological directions to identify actions and measure their impact in the specific context of the Web. Research on Information Warfare on the Web is still at an early stage and the question of the true nature of cyberwarfare actions that target the Web needs to be answered on both conceptual and methodological levels. Existing research has proved that the Web is a new battlefield with specific strategic objectives, but research needs to create new assessment tools to validate the real impact of cyberattacks, especially when they target "soft" targets like Web sites or social media platforms.

(1) The term "Arab Spring" was first coined in 2005 by several authors in magazine's editorials (Christian Science Monitor, Der Spiegel, Foreign Policy). Dominique Moisi was the first author to entitle a column with "An Arab Spring?"

(2) Evgeny Morozov. "**The Net Delusion: The Dark Side of Internet Freedom**". (Public Affairs, U.S., 2011).

Our ongoing observation aims at showing that infowar evolves from one context to another, that new forms of cyberwarfare emerge with new tools and new usages to create and define new strategic opportunities.

1- Infowar on the Web

The Interdisciplinary Research Unit in Web Science (UIR) at Saint-Joseph University of Beirut (USJ) answered the 2006Web Science call for interdisciplinary research[3] to understand the Web and its impact on society, with a specific approach: the Web is one, but the experience is quite different depending on where you are in the world. This "contextual" dimension is almost inevitable when you observe the Web in the Middle-East. Cultures, languages, history and politics create distortions and alter the global trends of Web impact and usage. Web players in the Middle-East include cyber armies and non-states playerswho use networks, computers, protocols and HTML code to support their political advantages, protect their assets and control their populations and supporters. There seems to be no debate about the nature of these actions event if cyberattacks in the context of digitalinfowars are often considered as weapons of mass annoyance.

Our previous researches[4]-[5]on the use of the Web as a weapon to create strategic advantages in asymmetric conflicts provided the Web Science research community with original insights in what War on the Web could look like from a contextual point of view. The first context was the 2006 war between Israel and Hezbollah and we demonstrated at the time that the Web was deliberately used by belligerents as a strategic platform to gain strategic advantage through infowar. The second study aimed at understanding the rules of engagement on the Web in the tragic context of the Syrian civil war. Considered as the first example of "civil infowar", the Syrian war proved that the Web and Social Media platforms

[3] Stéphane Bazan and Christophe Varin."Web Science in the context of the Arab Near East". **Proceedings of the WebSci10: Extending the Frontiers of Society On-Line**, Raleigh, NC: US, April 26-27th (2010).

[4] Sabrine Saad et al. "Asymmetric Cyber-warfare between Israel and Hezbollah": The Web as a new strategic battlefield". (Paper presented at the ACM WebSci'11, Koblenz, Germany, June 2011).

[5] Sofia El Amine et al. "Infowar in Syria: The Web between Liberation and Repression." (Paper presented at the ACM WebSci'12, Evanston, USA, June 2012).

could easily be transformed into battlefields to make strategic gains: the regime used fake accounts and deception techniques to identify rebels, denature their claims and create confusion. These actions had direct impact on the ground: arrests, torture and physical elimination. We also witnessed in this context the first official recognition by a state leader that his regular army was supported online by an "Electronic Army", the first of its kind in the region. The structure of the Internet access in Syria and the open and distributed nature of the Web helped this army to invade the virtual space to wage a war against online mobilization: the previous lessons of Tunisia and Egypt[6]were learned by the Syrian regime.

Information warfare in its broadest sense is "a struggle for the information and communications process, a struggle that began with the advent of human communication and conflict". It also can be defined as the "application of destructive force on a large scale against information assets and systems, against the computers and networks that support the four critical infrastructures (the power grid, communications, financial, and transportation)"[7]. Existing research on infowar raises more questions than provide answers. From Sun Tzu and Clausewitz to more recent definitions of digital wars, information operations (IO) or computer networks operation (CNO), information warfare is a catch-all concept and "scholars should improve the research agenda on CNO to include more rigorous studies and thus contribute to reversing the hype and misinformation that now surrounds such important topic"[8].

On a fundamental level and following Thomas Rid’s clarion call that "cyberwar will not take place"[9], there is a growing debate on the nature of "electronic wars". Erik Gartzke talks about the "myth of cyberwar" [9] and explains that "studying what could happen in cyberspace (or anywhere else)

[6] On the 28th of January 2011, Organisations that track global internet access detected a collapse in traffic in to and out of Egypt at around 10.30GMT. The shut down involved the withdrawal of more than 3,500 Border Gateway Protocol (BGP) routes by Egyptian ISPs, according to Renesys, a networking firm.

[7] Vernon B. Lewis. **Information Warfare and the Intelligence Community**. Final Report of the Snyder Commission. 1997.

[8] Giampiero Giacomello, "Measuring Digital Wars: Learning from the experience of peace research and arms control". **Infocon Magazine** Issue 1.Accessed June 13, 2014. http://www.iwar.org.uk/infocon/

[9] Thomas Rid, "Cyber War Will Not Take Place". **Journal of Strategic Studies**, 35-1 (2012): 5-32.

makes little sense without considering how Internet conflict will accomplish the tasks commonly addressed by terrestrial warfare. To supplant existing modes of conflict, cyberwar must be capable of realizing the political objectives, to which force or threats of force are commonly applied, something that in important respects, cyberwar fails to do. Cyberwar is much more likely to serve as an adjunct to, rather than a substitute for, existing forms of political violence. Indeed, rather than threatening existing hierarchies, cyberwar appears much more likely to augment the military advantages of status quo powers"[10]. If authors do not agree on the definition of infowar, they all agree that most countries did have an "awakening" at some point in recent times and "are only now beginning to see attempts to deal with the inherent vulnerability in critical infrastructure and government military networks"[11].

1.1 The Web as a multiplier effect

A second level of complexity comes with the technical nature of infowar and raises the following question: does cyberattacks target the Web or is the Web just another collateral asset to multiply the effect of larger scope objectives? To answer this question, we need to make a clear difference between cyberattacks and warfare actions that target the communication structure (the Internet) and infowar tactics on the Web itself. This distinction was clearly illustrated by the famous "weapons of mass annoyance" notion phrased by Stewart Baker[12] and explained by James Lewis: "*Much of the early work on the 'cyber threat' depicted hackers, terrorists, foreign spies and criminal gangs who, by typing a few commands into a computer, can take over or disrupt the critical infrastructure of entire nations. This frightening scenario is not supported by any evidence. Terrorist groups like Al Qaeda do make significant use of the Internet, but as a tool for intra-group communications, fund-raising and public relations. Cyber terrorist could also take advantage of the Internet to steal credit card numbers or valuable data to provide financial support for their operations. Cyber-terrorism*

[10] Erik Gartzke, "The Myth of Cyberwar". **International Security**, 38-2 (2013): 41-73.

[11] Richard Stiennon, "There is no cyberwar the way there is no nuclear war". **Forbes**. November 2011.

[12] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats". **Publications of the Center for Strategic and International Studies**, December 2002.

has attracted considerable attention, but to date, it has meant little more than propaganda, intelligence collection or the digital equivalent of graffiti, with groups defacing each other's websites. No critical infrastructures have been shut down by cyberattacks".

1.2 Identification and measure

The third level concerns methodology: how do we measure infowar, in terms of types of actions, frequency and efficiency? A 2003 paper by Giacomello[13]suggests that it should be possible to measure cyberwars. "In democratic countries, it should even be possible to compare different measurements and include the public in an open discussion. But research on digital wars takes place in closed laboratories and feeding public opinion with unverifiable data and the media with "*ad hoc*" anecdotes seem common developments in several countries".

The main questions behind infowar research lie in the difficulty to observe and independently measure it: like any information related to strategic issues, data is scarce and most of the sources use deception techniques or amplification of assessment, in order to guarantee efficiency. Many authors [8, 9] are questioning the reality of infowar, due to the lack of independent scientific tools to evaluate the true impact of cyberattacks.

1.3 The Break Things, Kill People rule and infowar on the Web

The pivotal aspect of the nature of infowar resides in the capability of the attack to transform the balance of forces or imply destruction or killing of human beings. To define infowar on the Web, we need to delimitate what we call "the Web": Should we just consider the Web as a set of technologies (Hypertext, HTML, URLs, browser and HTTP servers) brought together by Tim Berners-Lee in 1990 or do we need to extend the Web to all kind of human activities created with it? A cyberattack could indeed reduce our capacity to link, share and post, learn or be informed of a situation through web sites by denying access to a server or limiting a server's capacities.

In the context of the cyberwar in the Middle-East, official telecommunication structures are heavily controlled by public stakeholders: they control access to

[13] Giampiero Giacomello, **Measuring Digital Wars**.

information through the public networks and security services-owned proxy servers[14]. Limiting access to foreign or independent information by technical means should be considered as an act of cyberwarfare, even if it doesn't imply the "offensive" intention of a cyberattack. But for different approaches that might consider the strict military definition of CNO, this type and many other types of cyberattacks on the Web do not fall under the "break things and kill people" rule (BTKP)[15]. This includes psychological warfare (PSYOP), open source intelligence, Web page defacement or hacktivism. These actions could give a strategic advantage to a belligerent that might eventually lead him to victory, but this situation is highly improbable.

Infowar on the Web appears in certain contexts and seems to have different strategic objectives than the more "traditional" examples of cyberattacks (DDOS, viruses, worms, Man in the Middle, etc.). Subnational, transnational and supranational organizations and groups[16] have a preference for Web targets: the visibility they provide and their relative harmlessness is a best choice for them, in strategic terms. Nevertheless, the violent nature of infowar on the Web might be observed in its ability to disrupt normal assessment of a situation by critical players, like the financial system or political decision. Deceptive content, alteration of data or information could lead to misreading of events and wrong decisions.

1.4 Measuring infowar

Major contributions to the subject were outlined in Giacomello's paper[17]. The author presents the example of "missions of peace" researchers who needed to provide dependable data "as counterbalance to the views expressed by national security communities and military analysts". Today, most of the data available on infowar operations comes from two main sources: the intelligence community

[14] Stéphane Bazan et al., "Web Science in the context of the Arab Near East". **Proceedings of the ACM WebSci'10: Extending the Frontiers of Society On-Line.** Raleigh, NC: US (2010).

[15] Giampiero Giacomello, **Measuring Digital Wars**.

[16] Marvin Kalb and Carol Saivetz, "The Israel-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict". **The International Journal of Press/Politics,** 12-3 (2007): 43-66.

[17] Giampiero Giacomello, **Measuring Digital Wars**.

(mainly built around state structures or official think tanks and research centers) and hackers using specialized forums or Darknet sites to promote the technicalities of their achievements. Both sources have their own agendas and their information cannot be fully trusted. Furthermore, the growing number of states and non-states players involved in these actions like Anonymous or other groups, forms an unclear landscape: links or cooperation between players and cross-claimed actions make it really difficult to identify attacks and relate available data. Measuring infowar would need independent observers to validate:

1) The existence of the action, by identifying qualitative traces or quantitative distortions in usage,
2) A clear reading of the strategic intention by following available web content,
3) The availability of technical means in the hands of the attackers and
4) A precise evaluation of the damage done. Such a dataset would of course indicate the context of the attack, if related to direct conflict on the ground, or if the attack is just another event in an ongoing cyberwar.

It would also indicate if state and non-state players are involved in the attack: some countries might not have the technical proficiency to conduct certain types of attacks; meanwhile non-state players may need to regroup capabilities to perform actions more efficiently. Existing Web Science research could also be used to shed a new light on the reality of infowar: research methods related to trust (Metaxas 2010, O’Hara 2011, Vafopoulos 2011), gatekeepers and filtering (Jürgens et Al. 2011), cybercrime (Yip, 2011, Sugiura, Weber, 2012) and the Web observatory project [(18)] would eventually provide models and tools to store, analyze, "validate and interpret the data to advise industrialists, policy makers and the wider public as to its true significance". Finally, new research directions suggest that in the context of infowar, we might detect the creation of cyberwarfare Social Machines where players and crowds interact in various defensive or offensive ways.

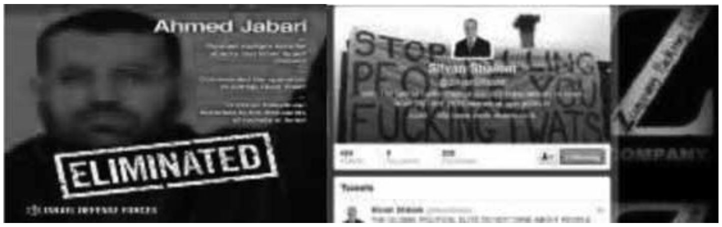
2 - The new rules of asymmetric infowar in the Middle-East

An asymmetric war is a conflict opposing two unbalanced forces, most of the time a state against a non-state player. In this context, non-conventional methods are used, and Web-related actions are progressively considered as

[(18)] http://wstweb1.ecs.soton.ac.uk/?page_id=1637 a new generation of weaponry. If the Web started as a hypertext network of information, it has become a network of socially organized people within virtual borders and turned into a useful tool to organize efficient aggression, repression or surveillance. Future conflicts in theMiddle-East will systematically be defined by the use and the exploitation of these new non-conventional and asymmetric methods of aggression and counter-aggression. For example, during the first year of the upraising, 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. But strategic efficiency is still difficult to evaluate: worldwide online coverage of atrocities committed by the regime has not provided the expected reaction by the international community and deceptive content provided by a disorganized opposition raised confidence doubts.

2.1 A new context: 2012 war in Gaza

Like in a classic warfare situation, belligerents learn strategic lessons from previous examples and the conflicts of 2006 in Lebanon and 2011 in Syria provided testing grounds for developing efficient response to asymmetric aggressions on the Web. In 2012, the short war between Israel and Hamas in the Gaza Strip brought new dimensions to infowar on the Web and its social media platforms. These new rules of asymmetric infowar could be described using Bertrand Boyer's typology of "the geopolitical players in cyberspace": the first type being the "traditionalplayerr" of asymmetric geopolitics such as state and non-state players, whereas the second type is the "emerging" born within Cyberspace[19].



[19] Bruno Boyer, "Le cyberespace, nouveau champ pour la géopolitique?", **Stratégie dans le cyberspace**. Iris, Observatoire Géostratégique de l'information, 2012.

2.1.1 Traditional players

Following its tradition of efficiency in intelligence actions, Israel is today a major player in the infowar and one of the most influential players in cyberwarfare. The cyber dimension of warfare has officially been integrated in the Israeli defense strategy since the last conflict with Hezbollah in 2006. Preparing electronic warfare is among priorities of the Israel Defense Forces (IDF). They sat up a military cyber command and opened a cyber-defense department. Moreover, the Official Israel Defense Forces spokesperson, AvitalLeibovich, (Head of International Media and Communication Branch, IDF Spokespersons Unit) became the director of the department "Interactive Media IDF" just after the Israel-Gaza 2012 conflict. Whereas usually very discreet about their operations, Israeli forces decided to communicate massively via social media tools in the Israel-Gaza conflict[20].

Facing the threat of cyberwar from Israel, Hamas, the Islamist organization that governs the Gaza Strip and its military wing, the Izz ad-Din al-Qassam Brigades, has certainly yield in a more traditional war against Israel, but has also sought to use infowar techniques through the Al-Qassam Cyber Fighters. Hamas attempted to conduct deception attacks consisting primarily of fake -mails and Facebook postings. For example, many Israeli citizens received false announcements from an "IDF Spokesman" warning that "if you opened these messages, terrorists in Gaza can geo-localize you" and "direct their Katyusha rockets at your location"[21].

2.1.2 Emerging players

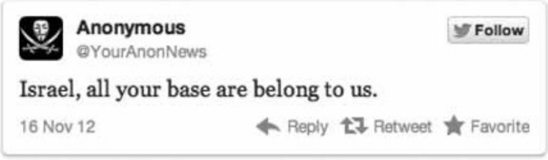
The concept of "citizen journalism" is an alternative and activist form of news gathering and reporting that functions outside mainstream media institutions. With foreign press not allowed entering the war zone, scarce electricity and very little Internet access infrastructure, the media dynamics in Gaza centered on a

[20] Liz Klimas, "Israel and Hamas Engage in Social Media War". **Blaze**, November 2012. Accessed June 13, 2014. http://www.theblaze.com/stories/2012/11/15/israel-and-hamas-engage-in-social-media-war/

[21] David Shamah, "Hamas launches email assault". **Times Of Israel**, November 2012. Accessed June 13, 2014.http://www.timesofisrael.com/hamas-script-kiddies-send-israelis-threatening-email-messages/

handful of independent Palestinian journalists who worked with a large range of media formats to provide footage and primary reporting for traditional and new media alike. One of these emblematic citizen journalists is SamehAkramHabeeb. During the conflict, Habeeb was constantly updating his "Gaza Today" blog[22], which included a daily report with news and photos.

Another emerging actor in the asymmetric infowar is Anonymous[23], the collective name of loosely-affiliated individuals that participate in hacktivism. Anonymous strongly opposes Internet censorship and surveillance and has hacked various government websites in many countries. It has also targeted major security corporations all over the world. On November 15th 2012, Anonymous began shutting down Israeli websites and launched the OpIsrael campaign. They attacked many Israeli websites in response to the IDF offensive in Gaza and claimed to have taken down at least 700 sites in less than 2 months. Using defacement tactics, they replaced webpages with messages condemning the Israeli campaign and expressing support for the citizens of Gaza.



Anonymous
@YourAnonNews

Israel, all your base are belong to us.

16 Nov 12

2.1.3 New Tools

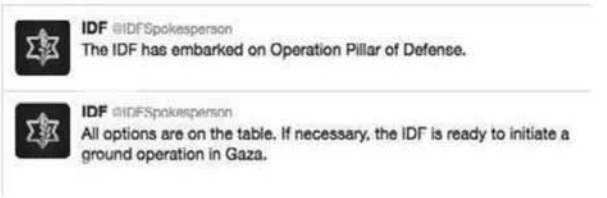
Israel’s attack on Gaza opened a new chapter in the use of the web as a weapon for infowar. Both parties have resorted to tools underexploited so far within the context of conflicts in the Middle-East, like Twitter, YouTube or Instagram. The use of these new platforms is characterized by dualism in strategic definition, with, on one hand, official accounts belonging to official authorities and, on the other hand, social media individual profiles used to network and socialize. Impact is very high, but deceptive content added by the enemy could ruin users’ confidence and trust.

[22] ***From Gaza***: Suffering In Stories, Features, Articles and Photos. Accessed June 13, 2014. http://gazatoday.blogspot.com

[23] Anonymous Group. **# Op Israel – Anonymous stands by Palestine in this time of war and grief**. Accessed June 13, 2014.http://anonrelations.net/anonymous-opisrael-95/.

2.1.3.1 Official accounts

For the first time in the Israeli-Arab infowar, traditional players have created official accounts to get their message through. The platform that was mostly used during this conflict is Twitter, with two official accounts @IDFSpokesperson and @alqassambrigades, for both mainplayers of the conflict. The IDF also started a string of Hashtags that were used quite extensively, with #pillarofdefense tweeting 88 tweets in just two days.



IDF @IDFSpokesperson
The IDF has embarked on Operation Pillar of Defense.

IDF @IDFSpokesperson
All options are on the table. If necessary, the IDF is ready to initiate a ground operation in Gaza.

The Al-Qassam Brigades, on the other hand, was quite reactive. They directly answered to IDF several times, by confirming the death of one of their senior operative, and furthermore by threatening the IDF and telling them that they have "opened the gates of hell". Both parties have also used other platforms to put forward their narrative, one of the most flagrant being the video posted on YouTube of the attack that lead to the death of Ahmad Al Jabari and the string of commentaries that followed from supporters of each side.

2.2 New Rules of engagement

In the aftermath of a "social media spying scandal", the IDF has bared most of its elements from using social media platforms and share information that may be deemed of military nature: Two years ago, a few IDF personnel had Facebook friends that where in fact covert Hezbollah operative who were able to monitor their movements and deployment through their social media feeds.

2.2.1 The "Terms of service" rule

Using Web platforms as new virtual conflict zones raises questions about the publications' content on the web. Most platforms are under increasing pressure from national legislations to bar heinous discourse. This didn't prevent the posting of the video of the attack on Ahmad Al Jabari by the IDF.

This example raises the following question: What kind of civic responsibility does social media platforms have in the Middle-East situation; particularly in preserving its users' autonomy and privacy? Facebook states in its community standards that: "Safety is Facebook's top priority. We remove content and may escalate to law enforcement when we perceive a genuine risk of physical harm, or a direct threat to public safety. You may not credibly threaten others, or organize acts of real-world violence. Organizations with a record of terrorist or violent criminal activity are not allowed to maintain a presence on our site[(24)]". Groups like The Syrian Electronic Army, officially supported and recognized by the Syrian regime, is still ostensibly present on the social network even after several attempts by Facebook to remove their account.

2.2.2 New targets and objectives

The 2012 conflict between Israel and Hamas is characterized by its increased visibility and official status on social networks. If this conflict has introduced the use of new mobilization tools, communication goals remain the same as those of a conventional war.

2.2.2.1 Legitimize / Delegitimize the War

For both Israel and Hamas, the main goal was to win the public opinion war on both national and international level. For Israel, the use of social media was an effective way to legitimize its military action against Hamas and explain "the morality of the war it is fighting"[(25)]: "There are two main goals of this IDF operation: to protect Israeli civilians and to cripple the terrorist infrastructure in the #Gaza Strip." — IDF (@IDFSpokesperson Nov. 14, 2012. For Hamas, the main goal was to delegitimize the Israeli attack on Gaza and show its violence by posting, for example, images of wounded or dead children: Alqassam Brigades @AlqassamBrigade : #Israel's military kills #Palestinian children in cold blood

[(24)] Brian Fung, "Does the Israel Hamas Internet War Violate Twitters Terms Of Service?" **The Atlantic**, November 2012. Accessed June 13, 2104. http://www.theatlantic.com/international/archive/2012/11/does-the-israel-hamas-internet-war-violate-twitters-terms-of-service/265285/.

[(25)] Michael Koplow, "How Not to Wage War on the Internet," **Foreign Policy**, November 2012. Accessed June 13, 2014. http://www.foreignpolicy.com/articles/2012/11/15/how_not_to_wage_war_on_the_internet in #Gaza,shelling civilians & populated areas #Humanrights pic.twitter.com/hTKX3sDs (picture of a dead child) 10:49 AM - 15 Nov 12.

2.2.2.2 Win the psychologicalWar

The use of online social media intensifies the degree of psychological warfare as these platforms become a virtual public sphere where the two parties can directly interact and influence each other. Israel and Hamas try to deepen the impact of what had been achieved against the enemy on the ground and boost the moral strength of its own troops and population by publicizing their military achievements. For example, the video posted by Al Qassam Brigades showing the launch of a Fajr 5 missile towards Tel Aviv for the first time revealed the will to weaken the confidence of the enemy. By directly threatening each other on social media platforms, in using the first-person plural personal pronoun "we" and the second-person personal pronoun "you", both sides compete in psychological warfare: IDF: "We recommend no Hamas operatives, whether low level or senior leaders, show their faces above ground in the days ahead. " The answer from Izz al-Din al-Qassam Brigades: "Our blessed hands will reach your leaders and soldiers wherever they are".

Using Internet social networks is a means to disseminate information quickly and directly to a mass audience. Both parties to the conflict bypass traditional media and tell the story straight to the audience. This is also known as "Hasbara" on the Israeli side(26).

2.2.2.3 Disinformation

Getting control of the narrative implies that, in this context, both parties delivered a message that is only deemed "productive" for their purpose(27). In advancing both their own agendas, the parties in conflict do not necessarily fully disseminate information. In this war, both parties have shown an eagerness to

(26) Chas Freeman, "Hasbara and Control Narrative as an Element of Strategy", **Middle East Policy Council**, December 2012. Accessed June 13, 2014. http://www.mepc.org/articles-commentary/speeches/hasbara-and-control-narrative-element-strategy

(27) "Israel Bans Social Network Use in Defense Forces", **The Journal**, October 2012. Accessed June 13, 2014. http://www.thejournal.ie/israel-bans-social-network-use-in-defence-forces-37010-Oct2010/?r_dir_d=1.

harness social media as one of their communication tools and therefore use social media as a platform to broadcast "a coherent message both in image and text, in support of the operational legitimacy"[28]. The contents posted can therefore be assimilated to propaganda as they are posted in conditions where each group tries to reply to the other without any trustful control of content.

Conclusion

Throughout this paper we have tried to demonstrate the innovative aspects of Infowar in the Middle East conflict. Israel developed a real infowar strategy, unlike in previous conflicts with Hezbollah in 2006 and with Hamas in 2009, which were dubbed as failures on the communication front. Indeed, it is clear that the IDF use of social media has evolved towards a more direct control of the communication and they have gradually and carefully built up their presence on social media platforms and established these platforms as key weapons in the state's public relations arsenal.Hamas did not have a real communication strategy; In fact they led a defensive and reactive infowar against Israel. Furthermore, we noticed the emergence of newplayers such as Anonymous or Citizen Journalists that were not previously involved in the Israeli-Arab "online" conflict.

Web Science research provides an innovative interdisciplinary approach to understand the impact of the Web in new contexts, like infowar in the Middle-East. The Web applications create infinite and ever-evolving practices that transform traditional political and social structures and re-organize power relations all around the World. To provide the scientific community with a correct assessment of how the Web might be used as a battleground or as a weapon of mass annoyance, infowar researchers need valid and reliable data to scrutinize, use multiple indicators and gather data from multiple sources. But a clear definition of the boundaries of infowar would also be needed, especially if we consider that the BTKP rule does not apply to the Web context. These preliminary steps could lead the way to the creation of resources of reference for research and real-time observation of the evolution of infowar on the Web… far from the hype.

[28] François Chauvancy, "War of Meaning, Cyberwar and Democracies". **Cyberspace and Information Warfare**. Ed. Daniel Ventre, Iste, Wiley (2011): 31-81.

References

Anonymous Group. *#OpIsrael – Anonymous stands by Palestine in this time of war and grief*. Accessed June 13, 2014.http://anonrelations.net/anonymous-opisrael-95/.

Bazan, S. and Varin, C., "Web Science in the context of the Arab Near East". *Proceedings of the ACM WebSci'10*: Extending the Frontiers of Society On-Line. Raleigh, NC: US (2010).

Boyer, B., "Le cyberespace, nouveau champ pour la géopolitique *?*", *Stratégie dans le cyberspace*. Iris, Observatoire Géostratégique de l'information, 2012.

Chauvancy, F., "War of Meaning, Cyberwar and Democracies". *Cyberspace and Information Warfare*. Ed. Daniel Ventre, Iste, Wiley (2011): 31-81.

El Amine, S. et al,. "Infowar in Syria: The Web between Liberation and Repression." Paper presented at the ACM WebSci'12, Evanston, USA, June 2012.

Freeman, C,. "Hasbara and Control Narrative as an Element of Strategy." *Middle East Policy Council*, December 2012. Accessed June 13, 2014. http://www.mepc.org/articles-commentary/speeches/hasbara-and-control-narrative-element-strategy

From Gaza: "Suffering In Stories, Features, Articles and Photos". Accessed June 13, 2014. http://gazatoday.blogspot.com

Fung, B., "Does the Israel Hamas Internet War Violate Twitters Terms of Service?" *The Atlantic*, November 2012.Accessed June 13, 2104. http://www.theatlantic.com/international/archive/2012/11/does-the-israel-hamas-internet-war-violate-twitters-terms-of-service/265285/.

Gartzke, E., "The Myth of Cyberwar."*International Security*, 38-2 (2013): 41–73.

Giacomello, G., "Measuring Digital Wars: Learning from the experience of peace research and arms control". *Infocon Magazine*, Issue 1. Accessed June 13, 2014. http://www.iwar.org.uk/infocon/

Lewis, J, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Publications of the Center for Strategic and International Studies, December 2002.

Kalb, M. and Saivetz, C., "The Israel-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict". *The International Journal of Press/Politics* 12-3 (2007): 43-66.

Klimas, L., "Israel and Hamas Engage in Social Media War". *Blaze*, November 2012. Accessed June 13, 2014. http://www.theblaze.com/stories/2012/11/15/israel-and-hamas-engage-in-social-media-war/

Koplow, M., "How Not to Wage War on the Internet". *Foreign Policy*, November 2012. Accessed June 13, 2014. http://www.foreignpolicy.com/articles/2012/11/15/how_not_to_wage_war_on_the_internet