Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a new strategic battlefield

Sabrine SAAD
UIR Web Science / CEMAM
Saint-Joseph University
Beirut, Lebanon,
+961 1 421 524
sabrine.saad@usj.edu.lb

Stéphane B. BAZAN
UIR Web Science / CEMAM
Saint-Joseph University
Beirut, Lebanon,
+961 1 421 524
stefan.bazan@usj.edu.lb

Christophe VARIN
UIR Web Science / CEMAM
Saint-Joseph University
Beirut, Lebanon,
+961 1 421 524
christophe.varin@usj.edu.lb

ABSTRACT
This study focuses on a particular context of conflict where Cyber-warfare has been used intensely and very frequently. The conventional war launched between the Israeli state and the Lebanese Shiite Party, Hezbollah, during the summer of 2006, was the scene of one of the most important acts of a wider virtual conflict, the Arab-Israeli Cyber-war, which started with the second Palestinian Intifada in 2000. The so-called "July War" has continued since 2006, and is being transposed from a conventional warfare context to a "permanent and ongoing Cyber-war", in terms of online information control and manipulation as well as repeated attempts to take technical control of official or influential Websites.

The study presents a detailed typology of the different kinds of attacks used by the two parties since the beginning of the conflict and a geopolitical analysis of their direct effect on the enemy's strategy. The goal of the study is also to demonstrate that future conflicts in the Arabic Near East will systematically be defined by the use and the exploitation of these new non-conventional and asymmetric methods, which purposes are to paralyze the military and civilian communication system of the enemy.

The proposed typology is based on three dimensions: 1) Cyber-attacks with strategic objectives that target Web information systems, communications and threaten civil security. 2) Cyber-attacks with technical objectives that target weapons control systems and military communication Websites. 3) Cyber-attacks with a political objective, which aim at altering the power balance in international diplomatic relations. The Web is an effective weapon for these kinds of attacks, but also represents a relatively easy target, mainly through distributed denial of service (DDoS) strategies. The study focuses on how the different players react to this Cyber-warfare, in terms of organized technical response. If their motivations follow the official speech of the Israeli state or that of Hezbollah, they are very diverse profile and skills, from young computer hackers to professional military actors.

The originality of our study is based on an interdisciplinary approach, mixing Web technology and geopolitics. It combines an observation of Cyber-warfare strategic issues with a purely technical analysis of the particular use of the Web in cases of Cyber-attacks between Israel and Hezbollah. It launches a debate on the efficiency of Web security systems implemented in Cyber-defense strategies and raises the issue of digital data vulnerabilities in future military and political conflicts.

Categories and Subject Descriptors
K.4 [**Computers and society**]

General Terms
Web Science

Keywords
Cyber Warfare, Information Warfare, Non-conventional warfare, Asymmetric conflict, International relations, Lebanon, Israel

1. INTRODUCTION
Information and communication systems are central in war strategies and Web interfaces are now widely used by military and intelligence institutions. It cannot be left apart while analyzing the belligerents' actions. It was borne out in 2006 between Israel and Hezbollah. Indeed, that war became a reference for the use of the Web in Arab Near East struggles, because of the intensity and variety of Web related cyber-attacks that were carried out before, during and after the "visible" military conflict.

Cyber-warfare is a series of techniques designed to acquire data and knowledge, and deprive the opponent of it, in a strategic purpose.[1] In its military meaning, it covers the "actions by a nation-State to penetrate another nation's computer networks for the purpose of causing damage or disruption."[2] The study presented here focuses on Web-related attacks, Web sites, Web applications and Web related communication and it aims at answering the following questions: How were these actions carried out in 2006? What are the main characteristics of the Cyber-warfare opposing Israel and Hezbollah? The Web opens new strategic perspectives and has become a significant battlefield. It requires proper techniques, and is henceforth used as a military tool.

2. THE STUDY

2.1 Context and goals

1 Francois-Bernard Huygue, "Cyberguerre et guerre de l'information, stratégies, règles et enjeux", under Daniel Ventre's supervision, 2010, introduction : « toute technique destinée à acquérir des données et connaissances (et à en priver l'adversaire) dans une finalité stratégique ». Lavoisier, p. 13

2 Richard Clarke, Robert K. Knake, "The next Threat to National Security and What to do About it", 2010

In July 2006, the Israeli army and the armed forces of the Lebanese Shiite party, Hezbollah, confronted in a thirty-four days long conflict. Classical means of action were used from both sides in this officially called "July War", but a new form of confrontation also played a major role: Cyber-warfare. The study aims at deciphering the strategic objectives that this new type of warfare can bring to the theatre of operations by analyzing the strategic dimensions of Cyber-attacks on the Web and the role of the different actors, civilians and institutions. By creating a typology of available choices in Cyber-attacks on the Web in this particular context, the study will emphasize the need to find new technical directions to protect Web applications and Web sites from their own vulnerability.

2.2 Methodology

If Cyber-warfare is largely studied and documented on technical and strategic levels, the very particular context of the Israeli-Hezbollah War of 2006 is still very sensitive and surrounded with secrecy. Strategies and clear explanations of what really happened during this war on the strategic battlefield of the Web are not documented, for the conflict is still active and actors cannot reveal their assets. The proposed study is based on existing literature, diplomatic reports and an inventory of testimonies of identified and revealed attacks from both sides. Web Science is about creating new methodologies to understand the impact of the Web and this study follows the proposals made for contextualized interdisciplinary analysis.

3. THE WEB AS A STRATEGIC TOOL

3.1 A new strategic field

3.1.1 Cyber-warfare: asymmetric and non-conventional warfare

According to Timothy Jordan, "technical tools have become the vehicle of wars' political and social issues". Indeed, his theory of "*technopower*"[3] states that war is no longer the conquest of new territories, but the destruction of the opponent's will to resist. What matters in current conflicts is the ability to discover and analyze the inns and outs before the adversary, in order to act faster. The Web is for this reason a major battlefield, since it is an endless source of information, offering new technical possibilities. Despite being borderless, the Web has obvious delimited "virtual territories" where citizens relate to content through national affiliation. Cyber-warfare is hence an asymmetric warfare that requires non-conventional means of action. An asymmetric war is a conflict opposing two unbalanced forces, most of the time a State against a non-State actor. In this context, non-conventional methods are used, and Web-related actions are progressively considered as part of that a generation of weaponry. The Web is a virtual territory, a virtual target. But it is also a direct tool of aggression, in terms of strategic content production and disinformation.

3.1.2 Actors implied

The study also shows that new forms of warfare imply the participation of several actors, human and institutional. Regarding the Web, it becomes much harder to distinguish between them. Indeed, the *Web Manifesto*[4] develops the concept of "Heterogeneous Networks". According to this theory, there is less and less distinction between the different actors, who gather in networks in order to reach specific aims. "We cannot imagine a social world independent from the material world […] The Web becomes a combination of human and non-human actors interacting in networks to produce particular outcomes."

In addition to that confusion between human, institutional and material actors, the distinction between militaries and civilians among human actors becomes thinner and thinner. The part played by civilians (as targets or aggressors) is reinforced, since the Web gives easier access to online activism. Moreover, military and intelligence institutions also use the new tools offered, and do not limit their actions to physical battlefields anymore. Indeed, the Web brings civilians and militaries closer, and some of them can now become cyber-soldiers or cyber-victims. That category comprises, regarding the July War, Israeli militaries, Hezbollah fighters but also computer specialists and hacker civilians close to the Party or just anonymous supporters. The study also reflects the variety of motivations behind every individual participating in larger Web activism leading to aggressive behavior on the Web.

3.2 Cyber-warfare objectives

3.2.1 Political strategy: communication and legitimization of actions

Information war does not limit itself to a national or regional frame. Hence, the Web was central in the belligerents' political strategies in 2006, since it enabled them to spread information worldwide. The direct "local" target can turn into a potentially global damage.

The study shows that regarding the conflict between Israel and Hezbollah, it is essential to communicate on a global scale because both of the States involved are characterized by important Diasporas. Their implication is part of the actors' political strategy. To reach that goal, the Web is a privileged mean to convey both sides' message. Through Web content dissemination, the opponents justify their actions in the eyes of the World. The Web is a communicational space allowing them to explain their objectives and their reasons to launch offensives or to retaliate. The Web is a convenient tool to legitimate war. It is indeed a strong ideological vehicle, and as such, a power issue. In 2006, psychological impact was as significant as physical destruction. Information and reputation were very strong weapons, and both parts needed to exercise moral influence on populations, and model public opinion, if they wanted to win the conflict durably.

3 Jordan, T. (2003). Technopower and its cyberfutures. In: Living with Cyberspace, Technology and Society in the 21th Century. Continuum, pp 120-131.

4 Halford, S., Pope C., Carr L, (2010). A manifesto for Web Science? In proceedings of Web Science 2010: Extending the frontier of Society On-line, April 26-27, Raleigh NC.

3.2.2 Influence strategy: modeling public opinion

In a struggle such as the July war, the ideological dimension is crucial. Hence, information war is at the chore of the actors' plan, and the Web has become its central instrument. It enabled Israel and Hezbollah to have an effect on public opinion's perceptions of the situation.

Psychological war took place on the Web through shocking pictures – dead children, destroyed buildings, bombings… The enemy is demonized, and "martyrs" are revered, in order to create hatred. On the one hand, Israel focused on making Hezbollah appear as a terrorist organization. On the other hand, Hezbollah used all available means to make sure that every piece of image and testimony was carefully controlled and edited for Web dissemination. For instance, it showed in the way the Lebanese party used the images of the Qana incident, where scores of civilians were killed after an Israeli bombing.

Propaganda is instigated to reach situational conscience. Campaigns are initiated by both camps, such as www.giyus.org, a Website launched by Israel, which aims at urging people to "give Israel their united support".

4. THE WEB AS MILITARY TOOL

The number of cyber-attacks types has considerably increased over the years. The threat is actually the sophistication of these attacks and the ability for a state or a group to initiate them efficiently and promptly. Classifying this high number of various attacks is a real challenge for the study. In fact, different taxonomies exist to identify the nature of an attack. An example of a generic taxonomy is to base it on the vulnerability used during an attack, the impact on the infrastructure, the target, the type of defense mechanism used and the informational impact.

4.1 Typology of attacks

4.1.1 Virus, malwares and Denial of Service (DOS) Attacks

The most dreaded attacks by Israel and Hezbollah are Denial of Service attacks and especially their distributed form (DDOS). This makes detection more and more difficult and the impact becomes stronger. These attacks originally exploit some weaknesses of Internet protocols which enable them to attack the infrastructure of the Internet like Web sites and Internet service providers. The DOS assault can be launched from a single computer but the attacker can also use the DDOS alternative where many computers (called Zombies) are used to start multiple flow attacks at the same time against the target.

In 2006, thousands of Israeli and Hezbollah hackers have attacked Websites with DDOS. Hezbollah hackers have hacked Israeli government and military Websites and in retaliation, the IDF managed to hack the strategic Website of the Hezbollah TV channel "Al Manar". Thus, Hezbollah was forced to use the Web server of the Quebecker company IWeb Technologies in order to find a new hosting solution for its Website. In the purpose of solving the problems of hosting its Websites after each attack, the party uses mobility and dissipation techniques.

Both antagonists have also sent viruses to Websites. The virus is able to infect the data of a computer as well as slowing down its performance. It has three stages, the first being the contamination stage as it is inserted in the target's Web server. This is accompanied with a contaminated target folder. When the folder is opened, the second stage begins, and the host Web server is infected. What was common was the appearance of messages, icons, and photos of dead children. For both Israel and Hezbollah, it has mostly caused modifications of informational content in official Websites and sometimes the shutdown of the Web server for hours. This period of unavailability can be used for a large strategic dissemination of content by the attacker, to gain substantial advantage.

4.1.2 Spying

The study also gathered evidence that Cyber-warfare on the Web includes the use of intentional intervention by opponents on Google Earth, a Web tool allowing visualization on Earth ground using satellite and aerial images, to hide or detect strategic assets of the enemy, as Hezbollah leaders' residences in Beirut, military areas in Israel or training camps of Hezbollah fighters.

4.1.3 Jamming and blocking

One of the most common techniques in such situations is penetration, interference and blockage. Indeed, Israel has tried to block Hezbollah's communication networks. They also have used their Warships moving about in the Lebanese territorial waters in order to interfere with Lebanese receivers and prevent the Lebanese from accessing the Web.

As for Hezbollah, it managed to penetrate the Israeli army's computers posted along the North frontier with Lebanon. They also tried to penetrate the Ministry of Foreign Affairs' network, the ministeries'offices and Israeli military camps networks.

4.1.4 Propaganda techniques

During the conflict, the Web was used by both sides as a tool of propaganda. Pro-Israeli organizations over the World have launched several campaigns of media influence on the Web. This coalition of Jewish and pro-Israeli organizations triggered the WUJS (World Union of Jewish Students) to provide a software called "megaphone" downloadable from the website. This Web software carries information alerts on the ongoing war and strategic messages on Israeli policy via official communiqués, online polls, discussion forums and blogs: the goal being to create live online reactions and create support for the Israeli actions. Therefore, they are supported by the Israeli Ministry of Foreign Affairs who encouraged the dissemination of this software.

5. CONCLUSION

Information war, and more specifically Cyber-warfare, was an essential aspect of the conflict that opposed Israel and Hezbollah in July 2006. In the context of Web Science and its interdisciplinary approach, this study focused on political, social and technical features of the belligerents' strategy regarding the use of the Web.

The Web has become a major battlefield in current struggles. The "July War" emphasized that Cyber-warfare gained in importance. Both actors became aware of that evolution. As a result, they improved their cyber-defense, understood as the set of means

available to counter cyber-attacks, in peace time as well as in war time.

6. REFERENCES

[1] Acosta D., (2007). The Makara of Hezbollah, Deception in the 2006 summer War. Naval Postgraduate School of Monterey, CA.

[2] Arpagian, N. 2009. *La Cyberguerre. La guerre numérique a commencé*. Institut d'Etude et de Recherche pour la Securité des Entreprises. Vuibert.

[3] Clarke, R.D. and Knake, R.K. 2010. *Cyberwar. The Next Threat to National Security and What To Do about It.* HarperCollins.

[4] Coleman, K. 2008. *Hezbollah's Cyber Warfare Program*. Internet Anthropologist Think Tank.

[5] Kalb Marvin, Saivetz, Carol. *THE ISRAELI-HEZBOLLAH WAR OF 2006: The Media as a Weapon in Asymmetrical Conflict.* Shorenstein Center on the Press, Politics and Public Policy at Harvard's Kennedy School of Government for presentation at the U.S.-Islamic World Forum in Doha, Qatar on February 18, 2007

[6] Michael, A. 2010. *Cyber Probing: The politicization of Virtual Attack. Israel chapter. Defense academy of the United Kingdom.*

[7] Osada,M. Baudot, M. and al.2007. *Illustration of Information Warfare. The Conflict between Israel and Hezbollah of summer 2006.* War Economic College.

[8] Ventre, D. and al. 2010. *Cyberguerre et guerre de l'information. Stratégies, règles, enjeux. Lavoisier.*