Infowar on the Web: When the Caliphate goes Online

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

Muriel Chamoun
UIR Web Science
CEMAM / FLSH
Saint-Joseph University
Beirut, Lebanon
muriel.chamoun@usj.edu.lb

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

ABSTRACT
The Middle-East has witnessed a tremendous increase in Information Warfare Operations on the Web in the last two years. The strategy developed by the ISIS group to increase visibility and reach takes advantage of various core competencies of digital media communication. By identifying actions and observing their impact in the specific context of the Middle East, this ongoing research tries to understand how ISIS conceived its Web communication strategy to target populations and spread its message to the online world.

Author Keywords
Cyberwarfare; Near-East; Information warfare; Strategy; Diplomacy; War; Social Media; Communication;

ACM Classification Keywords
K.4.1. Computers and Society: Public Policy Issues.

General Terms
Information Warfare; Middle East; Asymmetric Warfare;

INTRODUCTION
The Interdisciplinary Research Unit in Web Science (UIR) at Saint-Joseph University of Beirut (USJ) answered the 2006 Web Science call for interdisciplinary research with a specific approach: There is only one Web, but context should always be taken into account when trying to understand its impact on society [1]. Cultures, languages, available technologies and local politics create various distortions that significantly alter the Web's impact on society. Observing and understanding Information Warfare on the Web in the Middle East from a Web Science point of view requires a contextualized and interdisciplinary posture to fulfill the deficit of differentiation [2].

Our previous research - 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.

PREVIOUS RESEARCH AND METHODOLOGY
The first context was the 2006 war between Israel and Hezbollah, and we demonstrated at the time that belligerents deliberately used the Web as a strategic platform to gain strategic advantage [3]. 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 war on the Web", the Syrian war still proves that the Web and Social Media platforms could easily be transformed into battlefields to secure strategic gains [4].

Mixed research methods were used to provide the Web Science community with a contextualized landscape of Information Warfare in these various situations. Our methodology was presented in a short paper at the 6th ACM Conference. The "missions of peace" model, presented by Giacomello [5], was used to provide dependable data "as counterbalance to the views expressed by national security communities and military analysts." Our methodology follows a simple pattern: 1) Validate the existence of the action, by identifying qualitative traces or quantitative distortions in usage, 2) provide a clear reading of the strategic intention by following available web content, 3) identify the availability of technical means in the hands of the attackers and 4) formulate a precise evaluation of the damage done. The dataset also presents the context of the attack, if it's related to direct conflict on the ground, or if the attack is just another event in an ongoing Information Warfare.

A NEW CONTEXT
ISIS, (the Islamic State of Iraq and Syria) is a non-officially recognized state and a Jihadist group mostly operating in Iraq and Syria. It claims religious authority over all Muslims and aspires to a macro-state that would include several Middle East countries (Cyprus, Jordan, Kuwait, Israel, Lebanon, Palestine and part of Syria). The group is known for its overly rigid interpretation of Islam and its brutality and violence. ISIS is the product of discrepancy and inconsistency within Al-Qaeda and it used the beginning of Ramadan 2014 to declare itself the first Caliphate since the Ottoman Empire and its leader, Sheikh

Abou Baker Al-Baghdadi, the new Caliph for the global Ummah. In June 2014, ISIS began its offensive in northern Iraq and managed to conquer several cities that the Iraqi army immediately evacuated. In late June 2014, the Iraqi government lost control of its borders with Jordan and Syria.

OBJECTIVES

To structure the dataset, the 3-traits typology presented by HJ Ingram was used [6]. He uses three important traits of ISIS's information warfare to explore its central role in the group's strategy. One of the fundamental purposes of ISIS' information warfare is to create a polarization of the perceptions of its audiences and build strong support among the population they target to control. ISIS also uses information warfare "as the central strategic mechanism through which its politico-military activities are framed." As a third main trait, ISIS has demonstrated a deep strategic appreciation for its 'brand' as a symbol of its narrative and action.

BUILDING AUDIENCE AND SUPPORT

ISIS has developed a sophisticated online strategy that follows strict patterns: official online communication with a high visibility in social media (Twitter user @CtrlSec, identified around 11,000 accounts on Twitter tied to the Islamic state), SMS messages and less formal statements on events. Short videos are sent in almost real time (the "mujatweets") to provide the audience with ISIS' latest information. In parallel of this immediate communication, ISIS has supporting actors in online media such as *Markaz-al-Islam*, *Al-Haya*, *Al-Medrar*, *Al-Battar* where content is produced in a more blog-like, magazine-like style for specific audience building.

On another level, it has developed tools of its own, like the Android app "Dawn of Glad Tidings" to spread its message more efficiently [7]. This particular app allows the group's postings to be reposted on different websites, extending its reach to larger audiences. By using their supporters' networks, ISIS is more likely to target vulnerable individuals.

The full extent of ISIS's media ambitions can be seen in the output of its "Al-Hayat Media Center" [8]. Not to be confused with the Arab newspaper Al-Hayat, Al Hayat Media is specifically aimed at non-Arabic speakers, particularly younger viewers, and its output is closer to mainstream broadcast standards than anything else produced by Islamic groups so far. Like a conventional broadcaster, it has its own glossy indent, not dissimilar to that of Al-Jazeera: a teardrop-shaped logo of Arabic script materializing from a digital cascade of water. Its broadcasts invariably feature this logo or a fluttering black-and-white ISIS flag in the top corner of the screen. It makes programs in several languages – primarily German, English and French – as well as an hour-long "documentary" titled *The Flames Of War*, which was heralded by its own Hollywood-style trailer. ISIS also publishes audio content and an English-language PDF magazine, Dabiq, on its website. Issue two of this magazine likened the Caliphate to an "ark" in an apocalyptic "flood". It illustrated the analogy with images from the recent Hollywood epic, Noah.

Both PlayStation Network and the Sony Entertainment Network have been impacted by an attempt to overwhelm their websites with artificially high traffic which was later on claimed by ISIS's "*Lizard Squad*", a mysterious hacker group that has also previously claimed responsibility for a number of collective cyber attacks and operations including the taking down of the Vatican website. Sony later said on its PlayStation blog that the network had been taken down by a denial-of-service-style attack, which overwhelmed the system with traffic, but did not intrude into the network or access any of its 53 million users' information.

FRAMING POLITICO-MILITARY ACTIONS

ISIS has also proven to have more than just classic social media expertise. Many militants are believed to be high profile hackers and they threaten to launch 'massive' cyber attacks against the "Western Alliance" [9]. It has an official media wing, Twitter pages with direct messages issued by ISIS leadership and a fiery online magazine in English often containing disturbing images of mutilated bodies, death and destruction. In addition to that, ISIS has released many videos to show the beheadings of hostages and used them to gain political fights.

ISIS and their allied groups tried to launch major cyber attacks on Western Critical Infrastructure with the objective of setting up "digital Caliphate" [10]. It has demonstrated efficiency in keeping its "feeds" alive even when service providers shut down the accounts. For instance, the Cyber Caliphate, a hacker group claiming association with the group IS, seized control of the @CENTCOM Twitter and YouTube accounts that represent the U.S. Central military command. They tweeted a Pastebin message titled "*Pentagon networks hacked. American soldiers we are coming, watch your back. ISIS. #cybercaliphate*". The message included links to supposedly confidential US Army files. The hacker group also claimed taking control of the US media affiliates Fox and CBS News. They also hacked Newsweek's twitter account.

MARKETING THE CALIPHATE

The branding and marketing dimension of ISIS communication clearly appears as a strategic priority. The group needs to differentiate from other organizations like Al-Qaida or AQMI. The notion of Caliphate, is, especially in the Middle East context, an obvious tentative to build a clearly visible concept that supporters will identify as theirs and defend as a real territory.

DISCUSSION AND FURTHER RESEARCH

The two years old Information Warfare launched by ISIS on the Web used various strategies to build audience,

promote its politico-military actions and brand the concept of Caliphate. Our research has already identified hundreds of actions and as the fighting still rages in Syria and Iraq, we might see the development of other strategic dimensions, considering that ISIS is recently moving from a military action-oriented communication to a more "global terrorism-style" communication, following recent attacks in France and Tunisia.

REFERENCES

[1] Saad, S., Bazan, S., Varin, C. (2011) Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a new strategic battlefield. pp. 1-4. In: *Proceedings of the ACM WebSci'11*, June 14-17 2011, Koblenz, Germany.

[2] Anderson, J. Des communautés virtuelles ? Vers une théorie « techno-pratique » d'Internet dans le monde arabe. Revue Maghreb – Machrek 178 (Winter 2003-2004), 45-59.

[3] Saad, S., Bazan, S., Varin, C. (2011) Asymmetric Cyber- warfare between Israel and Hezbollah: The Web as a new strategic battlefield. pp. 1-4. In: Proceedings of the ACM WebSci'11, June 14-17 2011, Koblenz, Germany.

[4] El Amine, S., Bazan, S., Saad, S., Tesfa, A., Varin, C. Infowar in Syria: The Web between Liberation and Repression. In: Proceedings of the ACM WebSci'12, June 2012, Evanston, USA.

[5] Giacomello, G., 2003. Measuring Digital Wars: Learning from the experience of peace research and arms control. The Information Warfare Site Infocon Magazine Issue 1.

[6] Haroro J Ingram (2014) Three Traits of the Islamic State'Information Warfare, The RUSI Journal, 159:6, 4-11, DOI: 10.1080/03071847.2014.990810.

[7] ADL Web Site. 2014. Hashtag Terror: How ASIS Manipulates Social Media. Http://www.adl.org/combating-hate/international-extremism-terrorism/c/isis-islamic-state-social-media.html.

[8] Al-Hayat Media. 2014. There Is No Life without Jihad. Http://jihadology.net/2014/06/19/al-%E1%B8%A5ayat-media-center-presents-a-new-video-message-from-the-islamic-state-of-iraq-and-al-sham-there-is-no-life-without-jihad/

[9] Paganini P. 2012. What is ISIS and why it is menacing the world? Information Security Training Boot Camps. Http://resources.infosecinstitute.com/islamic-state-iraq-syria-isis-global-threat-analysis-effects-cyberspace-iraqi-situation/.

[10] Constine, J. 2014. ISIS "Cyber Caliphate" hacks U.S Military Command Accounts. TechCrunch Site. Http://techcrunch.com/2015/01/12/cyber-caliphate/.