



Contents lists available at [ScienceDirect](#)

## Public Relations Review



# Cyber warriors in the Middle East: The case of the Syrian Electronic Army



Ahmed K. Al-Rawi

Department of Media & Communication, School of History, Culture, & Communication, Erasmus University, Rotterdam, The Netherlands

### ARTICLE INFO

#### Article history:

Received 29 January 2014

Received in revised form 19 March 2014

Accepted 19 April 2014

#### Keywords:

Syrian Electronic Army (SEA)

Cyber War

Hactivism

Syria

Middle East

Political public relations

### ABSTRACT

This paper investigates the online hacking group, the Syrian Electronic Army (SEA), and examines its goals. The study argues that it is not a hacktivist group but is made up of cyber warriors who are closely connected to the Syrian government in order to serve two main goals: serving as a public relations tool for the Syrian government to draw the world's attention to the official Syrian version of events taking place in the country and countering the impact of Syrian oppositional groups. The study investigates the online reaction to SEA by analyzing the comments posted on its YouTube videos in order to better understand the group's aims and strategies and the public perception.

© 2014 Elsevier Inc. All rights reserved.

“Our grandfathers liberated Syria from colonialism and we, the Syrian Electronic Army, will protect Syria from the return of colonialism – Homeland. . .Honor. . .Loyalty”, YouTuber: [samisami70835](#)

## 1. Introduction: the Syrian Electronic Army (SEA)

Established around May 2011, SEA is a hacking group that claims to be independent from the Syrian government of Bashar Assad. Its old website ([syrian-es.org/](#)) is not functioning anymore due to US web service restrictions (Scharr, 2013). The Syrian Computer Society, which was established by Bashar al-Assad's brother Bassel in 1989 and was headed later by Bashar himself before becoming president, hosted and registered SEA's websites which indirectly show SEA's government affiliation (Scharr, 2013). On Instagram page ([instagram.com/official.sea/](#)), the first image that SEA has had was that for Bashar Assad, stating: 'Every year and you're the nation's leader' (as of 9 December 2013), yet on its Twitter page,<sup>1</sup> SEA describes itself as follows: “We are not an official side and do not belong to a political party. We are Syrian youths who responded to the call of duty after our homeland, Syria, was subjected to cyber attacks. We decided to respond actively under the name of Syrian Electronic Army SEA’ (The Syrian Electronic Army, 2013). It seems that the Syrian government felt an urgent need to counter the various cyber attacks against its websites, so it supported SEA. Aside from the hacking operations conducted by Anonymous, which is one of the well-known hacktivist groups in the world that supported free speech with the release of the Wikileaks cables and backed other popular protests like Occupy Wall Street, as explained below, other attacks included the email leaks by Syrian opposition activists who disclosed the emails of Bashar Assad and his close aides and family members which were

E-mail addresses: [alrawi@eshcc.eur.nl](mailto:alrawi@eshcc.eur.nl), [ahmed@aalrawi.com](mailto:ahmed@aalrawi.com)

<sup>1</sup> SEA has had 484 tweets and 10,183 followers as of 6 January 2014. The first tweet was sent on 31 July 2013.

published by *The Guardian* (Booth & Mahmood, 2012). Basically, it is impossible for SEA to operate inside the government controlled areas without the direct knowledge of and direction from the totalitarian government of Syria. Currently, SEA's new website ([sea.sy/index/en](http://sea.sy/index/en)) is operated from Russia which can be confirmed by the public email used which ends with .ru. In June 2011, Bashar al-Assad praised some of his supporters and highlighted the hacking operations of SEA, which he said "has been a real army in virtual reality" (Scharr, 2013).

According to its website, SEA attributes its existence to the anti-Assad stance taken by many Arab and Western media channels. SEA claims that these channels "started to support terrorists groups that killed civilians and members of the Syrian Arab Army as well as destroying private and public properties. These media outlets functioned as an umbrella for these groups to continue their acts by ignoring the coverage of terrorism in Syria and accusing the Arab Syrian Army to be behind everything. . . ." (The Syrian Electronic Army, n.d.). It seems that SEA's Facebook page has been routinely and continuously removed by Facebook administrators (The Syrian Electronic Army, 2013c). On its 252 Facebook page ([facebook.com/SEA.252](https://facebook.com/SEA.252))<sup>2</sup> that has been removed during the time this study was conducted, SEA wrote in the "About" section, three words to describe the group: 'Homeland. . . Honor. . . Loyalty' which is the same slogan used by Assad's Syrian Arab Army. By closely examining the 253rd Facebook page ([facebook.com/SEA.253](https://facebook.com/SEA.253)) that was created on 10 December 10, 2013 and removed shortly afterwards, one could notice that the page was heavily moderated by its creators and it only contained instructions on where to attack Syrian oppositional groups or report abuse or hate speech to Facebook administrators in order to shut them down.

Another Facebook page was created and was called 'The SEA Fourth Division' on 5 December 2013 which has had over 2546 likes in less than five days ([facebook.com/SEA.P.252](https://facebook.com/SEA.P.252)) and was shortly removed as well. One comment that was posted on 10 December 2013 mentioned that the Facebook page was being reported as one that violated Facebook guidelines; the person running the page instructed his followers to like or comment on some of its posts to avoid shutting it down, stating: "Please don't let me down, Shabiha". The term Shabiha is used for the militia members that are affiliated with Bashar Assad's regime. Other instructions were directed at hacking Facebook pages or reporting abuse in relation to Facebook pages that opposed Assad such as Al-Yarmouk Camp ([facebook.com/NewsOfYarmouk?fref=ts](https://facebook.com/NewsOfYarmouk?fref=ts)) and Imam Dhahabi Divisions ([facebook.com/kalidbrkat.ahmad.1](https://facebook.com/kalidbrkat.ahmad.1)). Later, SEA announced on its website that its 260th Facebook page was created:

They have been hurt by the blows of the SEA, so they fought us with everything that they have and shut down our Facebook page hundreds of times. Now, learn and let your masters learn, too. We swear that if you shut us down millions of times, you will neither affect our determination nor perseverance. This is our arena and you know this well. Wait for us for you who boast of freedom of speech. We do not need any funding from any side because there is only a need to have a computer and an Internet connection

*The Syrian Electronic Army (n.d.)*

Since it has been involved in a conflict for over three years, the Syrian government uses SEA as one of its public relations tools and cyberspace is just another battlefield. In the following section, an elaboration of the concept of cyber war is given.

## 2. Cyber war

Information warfare or cyber war is defined as 'aggressive operations in cyberspace, against military targets, against a State or its society' (Ventre, 2011, p. ix). Many governments around the globe are concerned about their cyber security and ability to (counter)-attack other adversaries. For example, Wikileaks cables revealed that the US government was pre-occupied with the growing cyber technologies and capabilities of some countries like China since Japan, its close ally, was far behind in the cyber war race (Wikileaks, 2009). The US government had also discussion and some kind of cooperation on cyber security with the Indian government (Wikileaks, 2004). This kind of concern is related to many governments' needs to obtain information that has security, economic, and political significance as well as to protect vital technology-related sectors from potential cyber-attacks which seem to be a regular occurrence. For example, the Algerian government introduced a new cybercrime bill in May 2008 after reports stating that government websites received about 4000 hacking attempts per month (International Telecommunication Union, 2012, p. 32). Some of the declassified documents of the US National Security Agency show that the US government planned to target "adversaries computers" since the year 1997. This was known as "Computer Network Attack" (CNA) which referred to "operations to disrupt, deny, degrade or destroy information in target computers or networks, 'or the computers and networks themselves'" (Richelson, 2013, paragraph 4). In many cases, cyber war is envisioned to be part of and an extension of a classical war. For instance, several hacking attempts were made against official Iraqi websites before the beginning of the 2003 war which resulted in defacing them and posting anti-Baathist messages by hackers from the USA (Al-Rawi Ahmed, 2012, p. 24 & p. 51). The war also led to various reactions including the hacking of nearly 20,000 websites between mid-March and mid-April 2003 that were either for or against the war on Iraq (Rojas, 2003). It is believed that some hacking attempts against government-run websites are either supported, indirectly encouraged, or at least tolerated by some governments. For example, an FBI informant once instructed some US hackers like Jeremy Hammond to attack certain targets in countries that were supposed to be allies with the US like Turkey, Iraq and Brazil (Cameron, 2013).

<sup>2</sup> The Facebook page was created on May 12, 2013 and has had 2779 likes.

According to the former secretary of State, Hillary Clinton, the US government hacked into websites run by al-Qaida's affiliates in Yemen and changed advertisements that bragged about killing Americans into pro-American advertisements (Hughes, 2012). In May 2007, a cyber war was initiated in Iraq to fight Iraqi insurgents. According to Bob Gourley, the chief technology officer for the US Defense Intelligence Agency, technology experts conducted "reconnaissance on foreign countries without exchanging salvos of destructive computer commands" (Harris, 2009). Yet, Iraqi insurgents themselves were believed to have hacked the US Predator drone video feed in order to disclose the kind of footage captured (Spillius, 2009), while other sympathizers with the Iraqi insurgency stepped up their war against US websites as a reaction against the US invasion of Iraq. For instance, the leader of the Tarek Bia Ziad Group, who is believed to be a Libyan hacker, managed to design a virus that infected many computers in the USA and the hacker attributed his action to his support for the Iraqi insurgency (Heussner, 2010).

Another recent example of cyber war is between Iran on the one hand and the USA and Israel on the other hand in relation to the controversial Iranian nuclear energy program. It is believed that the USA in coordination with Israel were allegedly involved in designing a malware, which is a malicious software, called MiniFlame whose aim is to steal information from specific targets in Iran as well as Lebanon in which Hezbollah operates. This malware has the ability to "remotely take screenshots of infected computers, record audio conversations that took place in the same room as the computer, intercept keyboard inputs and wipe data on command" (Ferran, 2012). Interestingly, the Flame virus that was created by the US and Israel was also found in Bahrain, Saudi Arabia, Qatar, and the UAE that are supposed to be close allies with the US (Flangan, 2012). Further, the US and Israeli governments were allegedly involved in designing Stuxnet 0.5 back in 2005 to attack Iran's Natanz enrichment facility (Arthur, 2013) which was followed by creating the Stuxnet worm that successfully disrupted and delayed the work of an Iranian nuclear facility (The Guardian, 2013; Valeriano & Maness, 2012). As a reaction, Iran allegedly cyber attacked several Persian Gulf oil and gas companies in Saudi Arabia and Qatar, according to US sources (Baldor, 2012).

The latest revelations by the former NSA's contractor, Edward Snowden, showed that the US government allocated a \$652 million budget for conducting 231 offensive cyber-operations worldwide back in 2011 (Gellman & Nakashima, 2011). Teams from the FBI, the CIA and the Cyber Command, the US military cyber operations, worked with the Remote Operations Center (ROC) to plan, administer, and supervise the work of "cyberwarriors" whose job was to "infiltrate and disrupt foreign computer networks" in countries like Iran, North Korea, China and Russia (Gellman & Nakashima, 2011). Other tasks included "locating suspected terrorists 'in Afghanistan, Pakistan, Yemen, Iraq, Somalia, and other extremist safe havens'" (Gellman & Nakashima, 2011). Snowden's revelations revealed numerous attempts to hack websites and computer networks in Europe and the Middle East including Al Jazeera TV channel's internal communications during George Bush's second term (Al Jazeera, 2013). In brief, several governments believe that obtaining sensitive online information from other countries and countering cyber attacks are of vital importance to their national security and Assad's government is certainly one of them.

### 3. Hacktivism & the Arab World

The word hacktivism is a combination of the words 'hacker' and 'activist' and was first coined by D.E. Denning who makes a distinction between cyberterrorism and hacktivism. Denning states that cyberterrorism refers to "the convergence of cyberspace and terrorism. It covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage. An example would be penetrating an air traffic control system and causing two planes to collide" (Denning, 2001, p. 241). On the other hand, hacktivism, refers to "operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are web sit-ins and virtual blockades, automated email bombs, web hacks, computer break-ins, and computer viruses and worms" (Denning, 2001, p. 241). In fact, it is difficult to distinguish between the two types of activities. The US government, for example, regards Anonymous as an illegal online organization. According to the US government, Anonymous is made up of "not-for-profit" cyber criminals (Snow, 2011) though the group is regarded by many as a hacktivist one. Weimann confirms that the line between the concepts of cyberterrorism and hacktivism is blurry as it is difficult to define the action of hacktivists attacking "national infrastructure, such as electric power networks and emergency services" (Weimann, 2005, p. 137). Weimann does acknowledge that cyberterrorism is done if some "nation states" are involved in hacking acts (Weimann, 2005, p. 141) and based on Denning's classical definitions, the Stuxnet worm can be regarded as an act of cyberterrorism since its aim was to "cause grave harm such as loss of life or severe economic damage".

One of Anonymous famous operations was called Syria – Fighting for Freedom that resulted in hacking the Syrian Customs website ([customs.gov.sy](http://customs.gov.sy)) (Anonymous, 2013). The Syrian Electronic Army reacted with hacking a Dutch website affiliated with Anonymous and posted a video to announce it, stating: "Our integrity is equivalent to the integrity of our territory. If you approached us even a little bit then you should await your complete annihilation" (YouTube, 2012a). One commentator on this video, MrKilian555, said: 'You will pay. Believe me. Expect us!' (YouTube, 2012a). As a reaction, Anonymous initiated operation #OpSyria that allegedly succeeded in exposing the names of five members of the SEA including, some of whom live in Romania and Russia and its leader who is known as Deeb (Murphy, 2013).

It is believed that Anonymous has many members from the Arab world. When the organization launched its #OpIsrael attack in November 2012, it managed to affect about 600 Israeli sites and released personal information that belonged to high-ranking Israeli officials (The Wire, 2013). In a newspaper interview with an Algerian member of Anonymous, he revealed a combination of nationalistic and religious motives behind the attack on Israeli websites. The Algerian hacker claimed that their mission was to 'wipe Israel from the map of cyberspace' in 2013 and that "details of over 20,000 Facebook and 5000

Twitter accounts and about 30,000 Israeli Bank accounts were released to the public” in #OpIsrael operation (Budihan, 2013). In the following section, the theoretical framework is introduced.

In this study, I argue that SEA is not a hacktivist group that defends or fights for some causes but is a community of cyber warriors who are defined as people “posses[ing] the characteristic of being sponsored by states and being subject to the oversight of their governments” (Baldi, Gelbstein & Kurbalija, 2003, p. 18). The Syrian government uses SEA as a public relations tool to serve its own interests, while the organization’s continuous denial of its strong connection to Assad’s regime has three main advantages. First, if SEA fails in its activities such as having its website hacked, no one can announce victory over the Syrian government but over a small hacking Syrian group. Second, this kind of vague link between the two “gives the Syrian government some protection from the legal and political consequences of SEA’s attacks” (Fire Eye, 2013). Finally, keeping the link to the Syrian regime ambiguous helps SEA’s organization in getting more recruits of the type of “script kiddies” or “Thrill Seekers” who seek fame and do not want to be associated with Assad’s government but are excited to be part of a ‘small’ organization that is sometimes able to attract the world’s attention.

It is important to note that SEA is not only made up of a group of cyber warriors who are supported by and affiliated to the Syrian government, but is also aided by what is called as “patriotic hackers” (Fire Eye, 2013) and “Thrill Seekers (or “cyberjoyriders”)” (Weimann, 2006, p. 41). In fact, SEA is a highly organized group despite the fact that it claims to work independently and with no clear organization. There is a well-defined leadership and hierarchy unlike the case of Anonymous which is made up of loosely connected networks of hackers from all over the world. For example, the TV channel, Al-Mayadeen, interviewed the leader of SEA on 26 September 2013 (YouTube, 2013c). The head of SEA, who is a young Syrian man living in Damascus, framed his group as hacktivists who are defending a cause, stating: “We have Syrian members who live outside the country in case the Internet connection is shut down. As an organization, we are proud to be on the same [FBI terrorist] list with that of the armed wing of Hezbollah” (YouTube, 2013c). This is also confirmed by Anonymous. When it initiated its #OpSyria operation, Anonymous hackers managed to disclose the identity of some SEA’s members living in Romania and Russia and its leader who is nicknamed Deeb (means wolf in Arabic) (Murphy, 2013). Finally, the pro-Syrian TV channel, Dunya, interviewed on 23 May 2011 a young Syrian man called Tareq who claimed to be the head of SEA and revealed that the group consists of hackers living inside the country and others in the Diaspora. Tareq emphasized that some Syrians living abroad are helping with translating the organization’s messages in different languages (YouTube, 2011b). Due to this hierarchical management, I argue that SEA is an organization that clearly exhibits public relations features serving the Syrian government for two main reasons. First, PR practitioners “must ensure their efforts support and contribute to the overall organizational goals and values”. SEA members are performing these services for the Assad government since they adhere to the same ideological beliefs and show great support for its political system. Second, those practitioners must show “confidence of top management in order to recommend needed adjustments to organizational policies and procedures” (Freitag & Stokes, 2009, p. 5). Again, SEA members largely act in this manner as the hierarchical structure is well established and respected.

In relation to its direct connection to the Syrian government, Reporters without Borders identified several countries that it called ‘Enemies of the Internet’ including Syria that uses the Syrian Electronic Army as an official intelligence tool. SEA is known to use malwares to collect information on oppositional groups (Reporters without Borders, 2013). These malware programs and Trojan applications include “Blackshades, DarkComet, Fynloski, Rbot, Xtreme RAT and Zapchast” and have “key logging, document and data stealing, and audio eavesdropping capabilities” (Fire Eye, 2013). For example, SEA published the names of 11,000 names and passwords of opposition members in July 2012 (Reporters without Borders, 2013, p. 33) and such information is sent to a “computer address lying within Syrian government-controlled Internet protocol (IP) space for intelligence collection and review” (Fire Eye, 2013). Also, SEA hacked and stole valuable information from Truecaller, Tango, and Viber which are all free Internet messaging and telephone services that are widely used by Syrian opposition members (Fire Eye, 2013).

It is important to note that most of SEA’s attacks are directed against the social media channels of traditional media outlets and as well as against Syrian oppositional websites and Facebook pages. This means that SEA is one of Assad’s international media and propaganda tools because after the beginning of the rebellion it has become difficult for the Syrian government to express its views to the world. There are numerous examples of SEA’s hacking operations that were mostly directed against Qatar, Saudi Arabia, USA, and the UK due to their political opposition to Assad’s regime. These attacks included hacking Al-Jazeera mobile and sending false mobile texts claiming that the Prince of Qatar was subjected to an assassination attempt (Associated Press, 2012). SEA also hacked the Facebook and Twitter accounts of Qatar Foundation in February 28, 2013 and posted messages indicating that Qatar supports terrorism (YouTube, 2013b). Tens of other media outlets like the Washington Post, the New York Times, and The Onion or their Twitter accounts that belonged to the Associated Press, NPR and Reuters were hacked by SEA. On the Associated Press Twitter account, SEA once wrote that the White House was bombed and that Obama got injured which made the stock market drop (Fire Eye, 2013; Memmot, 2013; Scharr, 2013). Further, one of the Twitter accounts that belong to BBC Weather was hacked by SEA that posted some sarcastic messages like “Earthquake warning for Qatar: Hamad Bin Khalifah about to exit vehicle” to ridicule his former obesity or “Hazardous for warning for North Syria: Erdogan orders terrorists to launch chemical weapons at civilian areas” (Deans, Plunkett, & Halliday, 2013). Other SEA hacking operations included distributed denial of service (DDoS), phishing, and domain name system (DNS) attacks with the case of the New York Times (Scharr, 2013).

SEA’s phenomenon prompted similar reactions from other countries that are close to Bashar Assad’s regime such as Algeria. For example, the “Algerian Electronic Army” appeared in 2013. On its Facebook page, a slogan similar to that used

by SEA is posted: 'Loyalty. ...Sacrifice. ...Commitment' ([The Algerian Electronic Army, 2013](#)). Another hacking group was created in 2013 called the "Tunisian Cyber Army" (TCA) ([The Tunisian Cyber Army, 2013](#)).<sup>3</sup>

#### 4. Theoretical framework

The theory used in this study is situated within the field of online political public relations, but it is important first to discuss the basic concept of public relations that is relevant to this study. In their typology of public relations, James E. Grunig and Todd Hunt (1984) introduced four public relations models including the press agency and the two-way asymmetric communications. The former is a one-way communication wherein "no dialog with the intended audience is required and the main objective is to put forward particular view of the world through the media and other channels" ([Edwards, 2009, p. 150](#)). This can be connected to the Syrian Electronic Army's main method of addressing the public which is through its website which does not contain any comments section. On the other hand, the aim of the two-way asymmetric communications is to "generate agreement between the organization and its publics by bringing them around to the organisation's way of thinking. Feedback from publics is used to adapt communications strategies to be more persuasive, not to alter the organisation's position" ([Edwards, 2009, p. 150](#)). This is similar to propaganda as the organization's goal is "to change only its target public" ([Sha, 2007, p. 8](#)) rather than itself which can be seen in SEA's use of its Twitter account, YouTube channels, and Facebook pages wherein feedback from the public is sent but there are no changes in SEA's strategies.

In relation to political public relations, the concept refers to "the management process by which an organization or individual actor for political purposes, through purposeful communication and action, seeks to influence and to establish, build, and maintain beneficial relationships and reputations with its key publics to help support its mission and achieve its goals" ([Stromback & Kiouisis, 2011, p. 8](#)). In the case of SEA, I argue that it is used as a political public relations tool because it helps the Assad regime in achieving some of its goals like building relationships and enhancing its reputation inside and outside Syria, which are some of the main functions of public relations ([Carroll & McCombs, 2003](#)). In his discussion of the image cultivation concept, Kunczik limits the goals of nation-state public relations efforts to "improving the country's image abroad" ([Kunczik, 2003, p. 400](#)), yet in the case of SEA, the national Syrian public is also a main target. This also corresponds with [Sriramesh and Vercic's](#) assertion that public relations does have an influence in "maintaining a particular political system" (2003, p. 5).

Theories on political public relations are rather new though the practice is as old as history ([Stromback & Kiouisis, 2011](#)). There is also a clear overlap and convergence in the concepts with many other terms like public diplomacy ([Signitzer & Coombs, 1992](#)). Copeland and Potter assert that public diplomacy is increasingly reliant on communication and information technologies because they are regarded as a "strategic asset that will play a more definitive role in determining the outcome of conflicts" ([Copeland & Potter, 2008, p. 279](#)). In fact, mediated communication in public relations is regarded as "tactical in nature" and is one of the three strategies used in public relations aside from interpersonal communication and social activities ([Sha, 2007, p. 9](#)). Another overlap that exists is between political public relations and propaganda as early PR theorists like Bernays, Lippman, and Lasswell admitted that persuasion and consequently propaganda are among the core elements of public relations ([Fawkes, 2009, p. 256](#)). For example, the father of public relations, [Bernays](#), once wrote that public relations is built on three elements: "informing people, persuading people, or integrating people with people" (1952, p. 12). In fact, public relations functions at different levels including what is termed as the "ideological PR" which is usually run by a state government such as the case of the Consultancy Bell Pottinger company that won 2.3 million Pounds to promote democracy in Iraq ([L'Etang, 2008, p. 19](#)). This can be linked to SEA whose objective is to serve as an ideological PR for the Syrian government.

Another dimension that is unique to this study is that SEA uses online public relations which "involves the use of Internet technologies to manage communications and to establish and maintain mutually beneficial relationship between an organization and its key publics" ([Hallahan, 2004, p. 587](#)). The traditional applications of online public relations include research, dissemination of information, queries, crisis response, discussion and debate, and relationship building. As indicated above, the latter is regarded as an "ultimate purpose" because it assists in enhancing "positive reputations (as a prerequisite to establishing positive relationships)" ([Hallahan, 2004, p. 591](#)). One of the main reasons behind the use of online and digital methods is that they have "the potential for developing" public relations with the publics "on a larger basis" ([Lordan, 2001; Sweetser, 2011, p. 309](#)). As SEA uses cyber technologies, its goal is to assist in Syrian government in its ongoing conflict by broadening the potential support as much as possible. This study aims at answering the following research questions:

RQ1: What kind of online rhetoric and sentiments are predominantly used by the online public?

RQ2: What is the tone of the online reaction toward the videos posted by SEA on its three YouTube channels?

#### 5. Method & results

For the purpose of this study, a webometric tool was used to mine the comments taken from three YouTube channels ([Thelwall, 2009](#)): 'syrianes0', 'syrianes1', and 'SEAOOfficialChannel'. These three channels belong to SEA since its Facebook

<sup>3</sup> On its Twitter page, TCA has 44 followers with a first tweet on 23 June 2013.

page gets removed continuously as explained above, so YouTube has become the only source where SEA's videos and accompanying comments are retained online. These three YouTube channels contain similar videos, but they are believed to be created in order to archive SEA's activities in case one of the channels is removed. 'syrianes1' was the first YouTube channel created by SEA on May 11, 2011 (YouTube, 2011a). It had 225 videos, 4436 subscribers, and 1,535,068 views as of January 6, 2014. The second YouTube channel is 'syrianes0' which was created on June 7, 2011. It had 285 videos, 2662 subscribers, and 1,100,823 views (YouTube, 2011c). Finally, 'SEAOOfficialChannel' had 42 videos, 218 subscribers, and 11,399 views and was created on April 9, 2013 (YouTube, 2013a).

In total, 536 videos were mined on 11 December 2013 which had a total views of 2,622,126, a total of 35.33 hours duration, 15,508 (47.5%) likes, and 17,093 (52.4%) dislikes. Amongst these videos, there were 134 ones with no comments, and the first video was posted on May 11, 2011, while the last one was posted on October 31, 2013. It is important to note that this webometric tool has limitation in mining comments due to YouTube API regulations, so not all the comments were mined; instead, the webometric tool mined 3019 comments that were content analyzed. The first comment was posted on May 11, 2011 while the last one that was mined was posted on December 8, 2013. From the identified and self-proclaimed geographic locations of YouTube users, we find, as expected, that the majority of commentators were from Syria 32.4% ( $n = 79$ ), followed by Saudi Arabia 27.5% ( $n = 67$ ), USA 13.5% ( $n = 33$ ), Pakistan 9.4% ( $n = 23$ ), Denmark 5.7% ( $n = 18$ ), and Canada 4.1% ( $n = 10$ ).

For the purposes of this study, all the comments that are written in Arabic, English, and Latinized Arabic were coded. There were very a few comments written in other languages, so they were removed from the study because the coders could not understand them. The first phase of coding revealed that 21.4% ( $n = 647$ ) of the comments were either irrelevant or cannot be understood. For the remaining 2368 comments, they were coded either as positive toward SEA and/or the Syrian government, or negative toward SEA and/or the Syrian government, or neutral in the sense that the commentator does not take a clear stance toward one of the sides and usually calls for calm and peace. Two coders who are native Arabic speakers and fluent in English coded 250 comments which was over 10% of the overall data investigated (Wimmer & Dominick, 1994, p. 173). Cohen's Kappa, which accounts for 'chance agreement', was employed since the data coded was nominal (Lombard, Snyder-Duch, & Bracken, 2002), and the inter-coder agreement test produced an agreement of .744 which was 'substantial' (Landis & Koch, 1977). The coding of the remaining comments revealed that 71.9% ( $n = 1703$ ) of the comments were pro-SEA, 25.3% ( $n = 601$ ) were anti-SEA, and 2.7% ( $n = 64$ ) were neutral.

## 6. Discussion & conclusion

The results of the study showed that there were 47.5% likes and 52.4% dislikes for all the videos posted on SEA's three YouTube channels. These figures reveal that there is a higher percentage of disapproval of SEA's videos mostly because of its obvious link to the Syrian government. In all the videos, there is not a single one that seems neutral toward the conflict since all of the clips blatantly side with and back Assad and his policies during the ongoing conflict. Yet, if we compare the results of the manual coding of comments with the number and percentage of the videos' likes and dislikes, we find a clear disparity which can be attributed to one possible explanation. The comments on SEA's YouTube channels are often but not always moderated. This is also supported by a few comments that mentioned that their anti-Assad's views were removed. For example, one YouTuber who seemed to be an Arab who hacked SEA's website called, TestMode21, mentioned the following: "You still remove comments without responding. You attribute the hacking attempt [against SEA's website] to the USA or Anonymous or whatever you imagine to cover your electronic defeat. . .". Another commentator, sary alsory, said: "What! Where's democracy? . . . Why do you remove the rebels' comments?". Further, on SEA's Facebook pages that are cited above, there were no anti-Assad or anti-SEA's comments which clearly indicate that the pages were always moderated on Facebook.

To answer the first research question: What kind of online rhetoric and sentiments are predominantly used by the online public? The results of the comment's analysis for the three YouTube channels run by SEA show a highly sectarian rhetoric which involved exchanges among people from inside and outside the Arab world. The video that had the highest number of views<sup>4</sup> showed a group of captive Syrian soldiers wearing civilian clothes being allegedly freed by Assad's army. The clip was taken from footage aired by the pro-Assad TV station, Al-Dunya, and most of the comments were mocking the film because of the allegedly fake production (YouTube, 2012c). This is followed by another video posted on the other channel 'syrianes1' in which the famous Syrian female singer, Assalah Nasri, refers to the Syrian national anthem and is framed as if she belittled it (YouTube, 2012b).<sup>5</sup> One YouTuber, Ali Ahmed, criticized Nasri saying: "You're vain. Go and practice sexual jihad with your great youth. . .". The reference to sexual jihad is repeatedly used by pro-Assad commentators to discredit opposing views. This was a controversial fatwa that was issued by some salafi – ultraorthodox Muslim sheikhs – and was rejected by the majority of Sunni imams that allows Muslim women to practice sex with the fighters as part of the efforts of establishing an Islamic state (BBC, 2013). On the other hand, hundreds of other commentators who oppose Assad and SEA often make references to 'Mutt'ah' which means 'pleasure marriage' that is a derogatory term used by some Sunnis to discredit the Shiite doctrine. The Alawite regime of Bashar Assad is regarded as an offshoot of Shiism, and the above term suggests that some Shiites are born as a result of illegitimate marriages (Haeri, 1989).

<sup>4</sup> It had over 870,000 views and over 1400 comments as of December 11, 2013 and was posted on 'syrianes1' channel.

<sup>5</sup> The video had over 1,045,000 views and 1174 comments as of December 11, 2013.

Further, one of the other popular terms used in the comments was the word ‘mule’ (Jahsh in Arabic) to refer to Bashar Assad whose name (Assad) means lion in Arabic; the mule is associated with stupidity and dullness unlike the ferociousness and bravery of the lion. For example, one YouTube user, kuwaitiCharisma, stated: “Bashar the mule, your end is near by God’s will”, and another YouTuber, shajkk, said: “God curse your soul Hafez for bringing this mule. He’s the excrement of lion”. Since the conflict in Syria has had regional implications that several other countries like Lebanon and Iraq, there were other political usages of the word Jahsh. For example, a Saudi film producer, Mohammed Al-Qahtani, announced his plan to make ‘Al-Jahsh’ film to depict the villainy and violence practiced by the Assad family throughout their rule. The Saudi film is planned as a reaction to making an anti-Saudi film called ‘King of the Sands’ by the Syrian director, Najdat Anzour, which was screened in several cinema theaters in Damascus and negatively depicted the life of King Saud of Saudi Arabia (Al-Qudus Al-Arabi, 2013). Further, the self-proclaimed geographic locations of the comments also indicate that people from different places inside and outside the Arab region are involved in the exchange of the sectarian language. As shown above, SEA reacted against the website of many Arab countries whose political stances opposed that of Assad’s government. Yet, various other hacking incidents were documented; for example, the website of the Iraqi Prime Minister, Nouri Maliki, was defaced and hacked by a group calling themselves “Team Kuwait Hackers” who compared him to Bashar Assad because of the Iraqi government’s support for Assad’s regime. The statement posted on Maliki’s website mentioned: “You want to be like Bashar Assad . . . Bashar is over” (Associated Press, 2013).

To answer the second research question: What is the tone of the online reaction toward the videos posted by SEA on its three YouTube channels? The results of the study showed that the majority of the comments 71.9% ( $n = 1703$ ) were Pro-SEA and/or pro-Assad. As mentioned earlier, there seems to be some kind of comments’ moderation. Most of these pro-SEA comments were directed at praising the hacking operations and Bashar Assad’s government. It is noteworthy to mention that there is a clear support by Syrians living in the diaspora and many other non-Syrian Arabs living in different parts of the world. This is also supported by the results of the geographic locations of the commentators. Amongst those sympathizers, there is a clear sectarian affiliation with SEA which is part of the Alawite – Shiite regime of Assad. For example, Hussein Al-Zubaidi, said: “Be victorious Bashar; all Shiites are under your service”, while ArmyShiaTeam, that seems to be another hacking group called SEA “heroes” and urged them to continue their efforts. Other comments were directed at demeaning Sunni Wahabis, Qatar, and Saudi Arabia due to their support for the Sunni rebels who are repeatedly accused of being terrorists, agents for Israel and the US, and mercenaries. Other commentators like Samer Al-Tariq from Iraq’s Karbala, harriwaltan from Germany, and Djesami algerien from Algeria all praised SEA and encouraged it to continue based on sectarian or nationalistic reasons.

Further, most of the Pro-SEA active commentators link the figure of Bashar Assad and his father Hafez with SEA. For example, the YouTuber, salem mhna, who seems to be a SEA member praises the group, saying: “We’re the eagles. . .our hearts are solid. . .going forward without withdrawing. . .We’re the falcons of Assad’s Syria”. In another post, he said: “SEA’s Facebook page was shut down 169 times and this is the 169th. The process will continue. . .Damn you, you’ll never pass and Syria will never kneel. We remain resolved until the established victory”. Also, there is a clear link made in the posts between Syria’s real army and its virtual one. For example, one YouTuber who seems to be a SEA member, sea Syria, says: “If you come on the ground. . .or by sea. . .or by air. . .or on the net, you will be crushed and your dreams will be squashed with it because we are more than you and are on the right side”. In addition, sami mhna, another YouTuber mentions: “Let God have mercy on the martyrs of the Arab Syrian Army, the doctrinal and electronic army”. Interestingly, some of the statements mentioned mimic those used by Anonymous in Style; for example, nahla ja, says: “I’m Syrian. . .I’m unarmed. . .I resist. . .I’m the Syrian Electronic Army”, while another YouTuber, SyrianLeaks2011, who appears to be a SEA member mentions: “We were not able to carry arms to protect our homeland, so we are here on this arena which is not less violent; we are certain of victory. . .”.

As for the anti-SEA and/or anti-Assad views, they constituted 25.3% of the total number of comments. Similar to the pro-SEA comments, the language used against SEA and Assad is highly sectarian and full of curses and insults. For example, one YouTuber, nasser35age, says: “The killer [Assad] is immortal in Hell’s fire. The day Syria saw you, there was nothing good but sectarianism and grudge”. Another YouTuber, MRaboFaisal1, used a sectarian language: “God curse you, Rafidah, and above all you dead Hafez, the shitty”. Here, Rafidah is one pejorative term given to Shiite by some salafis. Other users (goog50 and Al Dharif) wondered why SEA and Syria’s Assad asked help from Iran and Hezbollah to fight the rebels if they were truly strong enough to defend Syria alone. Hezbollah which means (God’s Party) in Arabic is repeatedly termed as (Lat’s Party). Here, Lat is a reference to one of the pre-Islamic polytheistic gods that Arabs used to worship and is intentionally replaced here in order to discredit the doctrinal basis of the Shiite Hezbollah. Also, the Shabiha and Syrians with pro-Assad views are often accused of being Iran’s proxies and are repeatedly called Bashar’s slaves or worshippers. Also, SEA is often mocked, while the validity of its hacking operations is either belittled or questioned. For instance, the YouTube user, AbuAlhassanSy, stated: “Let the kids [SEA members] play around on the net, while the adults are busy on the ground until the corrupt regime falls”, while, sourihorr, another YouTuber said: “This is the donkey’s electronic army” in reference to one of SEA’s hacking claims.

In relation to neutral comments, they constituted the lowest percentage (2.7%) as the majority of the comments were highly polarized. These comments encouraged peace and understanding and neither praised nor denounced SEA. For example, one YouTuber, a0562116637, condemned the violent language and sectarian rhetoric stating: “Based on these comments, I understand now why we are labeled as Third World countries”. Another YouTube user, abdul k hetar, said: “By God, I feel surprised by the kind of insults and curses I read. Is this the kind of moral standard held by the faithful Muslims?”.

In conclusion, the case of the Syrian Electronic Army can be applied to the several other totalitarian regimes, possibly like North Korea, that use cyber warriors as an online public relations tool either to steal information from opposition groups or hack websites and SNSs outlets aiming at creating an image of a sophisticated and undefeatable regime. This can be part of the cyber war tactics that are used for offensive and defensive purposes. SEA effectively used cyberspace to defend, support, and popularize the Assad regime, and some its strategies were unorthodox. It is crucial to mention here that SEA's case remains unique due to the special circumstances that led to its creation. Stromback and Kiousis emphasize the importance of examining the “cultural, social, political, institutional, or systemic context” (2011, p. 4) as well as the different “beliefs, values and attitudes” and “configurations of social, economic and political factors” (Edwards & Hodges, 2011, p. 3) that all play a major role in shaping the nature and goals of public relations efforts.

Further, the Syrian government uses cyber war is part of its tools to protect its own interests similar to other governments around the world. SEA is one of Assad's government means to attack vital targets in the cyber space that adds prestige and enhances an image of a sophisticated regime that is able to create havoc in the West. This image has an impact on the public relations efforts directed at the Syrian public in particular and the Arab and international public in general. The study showed that SEA is a highly organized group of cyber warriors whose goal is to serve Bashar Assad's government by either stealing sensitive information for intelligence purposes that can help in combating the Syrian rebel groups or hacking the websites of international media outlets or their social media channels in order to draw international attention to Assad's cause. SEA uses all the available tools at its disposal to spread the word on the activities of Assad's Syrian army and to distort the image of Syrian rebels which is similar to the general objectives of the official Syrian media outlets. It is reasonable to think that SEA's future will always be linked to the fate of Bashar Assad and his Baath government.

## Acknowledgement

I would like to thank my wife, Dr. Alaa Al-Musalli, for her kind assistance in conducting this research study as she was one of the coders in the pilot study.

## References

- Al-Qudus Al-Arabi. (2013 January). *After announcing the Al-Jahyesh film, Syrian authorities ban the entrance of all Saudi cars into the country*. Retrieved from <http://www.alquds.co.uk/?p=118920>
- Al Jazeera. (2013 September). *Report: US hacked Al Jazeera communications*. Retrieved from <http://www.aljazeera.com/news/middleeast/2013/09/20139113658335421.html>
- Al-Rawi Ahmed, K. (2012). *Media practice in Iraq*. Hampshire: Palgrave Macmillan.
- Anonymous. (2013 August). *Anonymous syria – fighting for freedom*. Retrieved from <http://vimeo.com/75158017>
- Arthur, C. (2013, February 26). Symantec discovers 2005 US computer virus attack on Iran nuclear plants. *The Guardian*, Retrieved from <http://www.theguardian.com/technology/2013/feb/26/symantec-us-computer-virus-iran-nuclear>
- Associated Press. (2012, September 9). *Al Jazeera says hackers sent false mobile texts*. Retrieved from <http://news.yahoo.com/al-jazeera-says-hackers-sent-false-mobile-texts-154921087.html>
- Associated Press. (2013, February 12). *Hackers call Iraqi PM 'oppressor' on his website*. Retrieved from <http://news.yahoo.com/hackers-call-iraqi-pm-oppressor-website-111725197.html>
- Baldi, S., Gelbstein, E., & Kurbalija, J. (2003). *Hactivism, cyber-terrorism and cyberwar: The activities of the uncivil society in cyberspace*. Msida: Diplo Foundation.
- Baldor, L. (2012, October 12). *US: Hackers in Iran responsible for cyberattacks*. Associated Press. Retrieved from <http://news.yahoo.com/us-hackers-iran-responsible-cyberattacks-072429280-finance.html>
- BBC. (2013, October 26). *Tunisia's 'sexual jihad' – extremist fatwa or propaganda?* Retrieved from <http://www.bbc.co.uk/news/world-africa-24448933>
- Bernays, E. L. (1952). *Public relations*. Norman, OK: University of Oklahoma.
- Booth, R., & Mahmood, M. (2012, March 14). *How the Assad emails came to light*. *The Guardian*, Retrieved from <http://www.theguardian.com/world/2012/mar/14/how-assad-emails-came-light?uni=Article:in%20body%20link>
- Budihan. (2013, April 10). *An Algeria Hacker narrates to Asharq Al-Awsat the details of the Cyberwar against Israel*. *Asharq Al-Awsat*. Retrieved from <http://www.aawsat.com/details.asp?section=4&issueno=12552&article=724133&feature=#.UqW4ZtK1zTo>
- Cameron, D. (2013, November 16). *Jeremy Hammond supporters share list of countries the FBI allegedly used him to hack*. Retrieved from <http://www.dailydot.com/news/jeremy-hammond-fbi-foreign-governments-list/>
- Carroll, C. E., & McCombs, M. (2003). *Agenda-setting effects of business news on the public's images and opinions about major corporations*. *Corporate Reputation Review*, 6(1), 36–46.
- Copeland, D., & Potter, E. H. (2008). *Public diplomacy in conflict zones: Military information operations meet political counter-insurgency*. *Hague Journal of Diplomacy*, 3(3), 277–297.
- Deans, J., Plunkett, J., & Halliday, J. (2013, March 21). *BBC Weather Twitter account taken over by Syrian regime supporters*. *The Guardian*, Retrieved from <http://www.theguardian.com/media/2013/mar/21/bbc-weather-twitter-syrian-regime>
- Denning, D. E. (2001). *Activism, hactivism, and cyberterrorism: The Internet as a tool for influencing foreign policy*. In J. Arquilla, & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239–288). Rand Corporation.
- Edwards, Lee. (2009). *Public relations theories: An overview*. In R. Tench, & L. Yeomans (Eds.), *Exploring public relations* (pp. 149–173). Essex: Pearson Education.
- Edwards, L., & Hodges, C. (2011). *Introduction: Implications of a (radical) socio-cultural 'turn' in public relations scholarship*. In L. Edwards, & C. Hodges (Eds.), *Public relations, society & culture: Theoretical and empirical explorations* (pp. 1–14). London: Routledge.
- Fawkes, J. (2009). *Public relations, propaganda and the psychology of persuasion*. In R. Tench, & L. Yeomans (Eds.), *Exploring public relations* (pp. 252–272). Essex: Pearson Education.
- Ferran, L. (2012, October 15). *Researchers: Cyber Attack MiniFlame Hit Lebanon, Iran*. *ABC News*. Retrieved from <http://abcnews.go.com/blogs/headlines/2012/10/miniflame-researchers-say-extremely-targeted-cyber-attack-hit-lebanon-iran/>
- Fire Eye. (2013, July 30). *Syrian Electronic Army hacks major communications websites*. Retrieved from <http://www.fireeye.com/blog/technical/cyber-exploits/2013/07/syrian-electronic-army-hacks-major-communications-websites.html>
- Flangan, B. (2012, June 5). *Sophisticated flame computer virus detected in UAE*. *The National*, Retrieved from <http://www.thenational.ae/business/industry-insights/technology/sophisticated-flame-computer-virus-detected-in-uae>
- Freitag, A. R., & Stokes, A. Q. (2009). *Global public relations: Spanning borders, spanning cultures*. London: Routledge.

- Gellman, B., & Nakashima, E. (2013, August 31). U.S. spy agencies mounted 231 offensive cyber-operations in 2011. Documents show. *The Washington Post*.
- Haeri, S. (1989). *Law of desire: Temporary marriage in Shi'i Iran*. New York: Syracuse University Press.
- Hallahan, Kirk. (2004). Online public relations. In L. Robert, & Heath (Eds.), *Encyclopedia of public relations* (pp. 587–592). California: Sage Publications.
- Harris, S. (2009, November 14). *The Cyberwar Plan*. *National Journal Magazine*. Retrieved from <http://www.nationaljournal.com/member/magazine/the-cyberwar-plan-20091114>
- Heussner, K. M. (2010, September 13). *Hacker Posts video claiming 'Here You Have' worm*. ABC News. Retrieved from <http://abcnews.go.com/Technology/anti-us-hacker-claims-worm/story?id=11624252>
- Hughes, D. (2012, May 23). *Hillary Clinton: U.S. hacked Yemen al-Qaida sites*. ABC News. Retrieved from <http://abcnews.go.com/blogs/headlines/2012/05/secretary-clinton-we-hacked-yemen-al-qaeda-sites/>
- International Telecommunication Union. (2012). *Connect Arab Summit 2012: Connecting the unconnected by 2015: ICT Adoption and Prospects in the Arab Region*. CH-1211 Geneva, Switzerland: International Telecommunication Union.
- Kunczik, M. (2003). Transnational public relations by foreign governments. In K. Sriramesh, & D. Vercic (Eds.), *The global public relations handbook: Theory, research, and practice* (pp. 399–424). London: Routledge.
- Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, 33(1), 159–174.
- L'Etang, Jacquie. (2008). *Public relations: Concepts, practice and critique*. London: Sage.
- Lombard, M., Snyder-Duch, J., & Bracken, C. C. (2002). Content analysis in mass communication: Assessment and reporting of intercoder reliability. *Human Communication Research*, 28(4), 587–604.
- Lordan, E. J. (2001). CyberSpin: The use of new technologies in public relations. In R. L. Heath (Ed.), *Handbook of public relations* (pp. 582–590). Thousand Oaks, CA: Sage.
- Memmot, M. (2013, April 16). *NPR.org Hacked; 'Syrian Electronic Army' Takes Responsibility*. NPR. Retrieved from <http://www.npr.org/blogs/thetwo-way/2013/04/16/177421655/npr-org-hacked-syrian-electronic-army-takes-credit>
- Murphy, L. (2013, September 4). Anonymous isn't ready to publish the identities of the Syrian Electronic Army—yet. *The Daily Dot*. Retrieved from <http://www.dailydot.com/news/anonymous-syrian-electronic-army-names/>
- Reporters without Borders. (2013, March 12). *Enemies of the Internet: 2013 Report*. Retrieved from <http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet-2013.pdf>
- Richelson, J. T. (2013, April 26). *National Security Agency tasked with targeting adversaries' computers for attack since early 1997. According to declassified document*. *National Security Archive Electronic Briefing Book No. 424*. Retrieved from <http://www2.gwu.edu/nsarchiv/NSAEBB/NSAEBB424/>
- Rojas, P. (2003, April 24). *The paranoia that paid off*. *The Guardian*.
- Scharr, J. (2013, September 1). What is the Syrian Electronic Army. *Live Science*. Retrieved from <http://news.yahoo.com/syrian-electronic-army-123906820.html>
- Sha, B.-L. (2007). Dimensions of public relations: Moving beyond traditional public relations models. In S. Duhe (Ed.), *New media and public relations* (pp. 3–26). New York: Peter Lang.
- Signitzer, B. H., & Coombs, T. (1992). Public relations and public diplomacy: Conceptual convergences. *Public Relations Review*, 18(2), 137–147.
- Snow, G. M. (2011, April 12). *Statement before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Washington, D.C. The FBI – Cybersecurity: Responding to the threat of cyber crime and terrorism*. Retrieved from <http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism>
- Spillius, A. (2009, December 17). *Iraq insurgents hacked Predator drone video feed*. *The Telegraph*. Retrieved from <http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/6834884/Iraq-insurgents-hacked-Predator-drone-video-feed.html>
- Sriramesh, K., & Vercic, D. (2003). A theoretical framework for global public relations research and practice. In K. Sriramesh, & D. Vercic (Eds.), *The global public relations handbook: Theory, research, and practice* (pp. 1–22). London: Routledge.
- Stromback, J., & Kioussis, S. (2011). Political public relations: Defining and mapping an emergent field. In J. Stromback, & S. Kioussis (Eds.), *Political public relations: Principles and applications* (pp. 1–32). London: Routledge.
- Sweetser, K. (2011). Digital political public relations. In J. Stromback, & S. Kioussis (Eds.), *Political public relations: Principles and applications* (pp. 293–313). London: Routledge.
- The Algerian Electronic Army. (2013, May 23). *Facebook*. Retrieved from <https://www.facebook.com/AlgerianElectronicArmy>
- The Guardian. (2013, June 28). *Former US general James Cartwright named in Stuxnet leak inquiry*. Retrieved from <http://www.theguardian.com/world/2013/jun/28/general-cartwright-investigated-stuxnet-leak>
- The Syrian Electronic Army. (n.d.). About. Retrieved from <http://sea.sy/index/ar>
- The Syrian Electronic Army. (2013a). *Twitter*. Retrieved from [https://twitter.com/Official\\_SEA16](https://twitter.com/Official_SEA16)
- The Syrian Electronic Army. (2013b, December 5). *Our Facebook Page number 260*. Retrieved from <http://sea.sy/article/id/2023/ar>
- The Syrian Electronic Army. (2013c). *Facebook*. <https://www.facebook.com/SEA.P.260>
- The Tunisian Cyber Army. (2013). Retrieved from <https://twitter.com/TN.Cyberarmy>
- The Wire. (2013, April 7). *Anonymous Hits Israel with a Massive Cyber Attack, Israel Attacks Back*. Retrieved from <http://www.thewire.com/global/2013/04/anonymous-hits-israel-massive-cyber-attack-israel-attacks-back/63969/>
- Thelwall, M. (2009). *Introduction to Webometrics: Quantitative Web Research for the Social Sciences*. San Rafael, CA: Morgan & Claypool.
- YouTube. (2011a, May 11). *Syrianes1*. Retrieved from <http://www.youtube.com/user/syrianes1/about>
- YouTube. (2011b, May 23). *The Good Morning Program on Dunya TV. . Thank you*. Retrieved from <http://www.youtube.com/watch?v=yZmMmTb6wQ>
- YouTube. (2011c, June 7). *Syrianes0*. Retrieved from <http://www.youtube.com/user/syrianes0/about>
- YouTube. (2012a, July 18). *Anonymous website hacked and defaced by SEA*. Retrieved from [http://www.youtube.com/watch?v=\\_EGqCjHm5JE](http://www.youtube.com/watch?v=_EGqCjHm5JE)
- YouTube. (2012b, July 28). *Assalah Nasri mocks the anthem of her home country and Tonny scolds her*. Retrieved from <http://www.youtube.com/watch?v=InmbgpaFGcQ>
- YouTube. (2012c, August 10). *The Video that made everyone who saw it cry – The Syrian Arab Army*. Retrieved from <http://www.youtube.com/watch?v=LnwfKBfDfXc>
- YouTube. (2013a). *SEAOfficialChannel*. Retrieved from <http://www.youtube.com/user/SEAOfficialChannel/about>
- YouTube. (2013b, March 1). *Hacking Qatar Foundation – SEA*. Retrieved from <http://www.youtube.com/watch?v=BCBWkNgBTZc>
- YouTube. (2013c, September 23). *Al-Mayadeen – From the ground – SEA*. Retrieved from <http://www.youtube.com/watch?v=gBRZRnzli3w>
- Valeriano, B., & Maness, R. (2012, November 21). *The fog of cyberwar: Why the threat doesn't live up to the hype*. *Foreign Affairs*. Retrieved from <http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar>
- Ventre, D. (2011). *Cyberware and information warfare*. London: John Wiley & Sons.
- Weimann, G. (2005). *Cyberterrorism: The sum of all fears? Studies in Conflict & Terrorism*, 28(2), 129–149.
- Wikileaks. (2004). *Indo-US cyber security forum preparatory consultations in New Delhi*. E.O. 12958. *US Embassy New Delhi*. Retrieved from <http://wikileaks.org/cable/2004/11/04NEWDELHI7026.html>
- Wikileaks. (2009). *SECNAV, GOJ officials discuss 'Unshakeable' alliance, China concerns*. *US Embassy Tokyo*. E.O. 12958. 27 August. Retrieved from <http://wikileaks.org/cable/2009/08/09TOKYO2002.html>
- Wimmer, R. D., & Dominick, J. R. (1994). *An introduction to mass media research*. California: Wadsworth.