Public Relations Review 40 (2014) 420–428

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
Hacktivism
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.

> "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 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,[1] 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, ahmed@aalrawi.com

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

http://dx.doi.org/10.1016/j.pubrev.2014.04.005
0363-8111/

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) 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)[2] 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) 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) 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) and Imam Dhahabi Divisions (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 if 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 preoccupied 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).

[2] The Facebook page was created on May 12, 2013 and has had 2779 likes.