

NOV  
2013

# Syrian Electronic Army (SEA) Targets Qatar



[TRADOC G-2 Intelligence Support Activity  
\(TRISA\)](#)

Complex Operational Environment and  
Threat Integration Directorate (CTID)





# OEA Team Threat Report



---

## Purpose

- To inform the Army training community of the Syrian Electronic Army (SEA) cyber attack on Qatari websites.
- To provide background information on the SEA.
- To describe the general motivation behind the SEA's attacks.

---

## Executive Summary

- The SEA is a disconnected group of Syrian IT professionals who are intent on combating what they view as unjust media coverage of the Syrian government and external support for the rebels.
- Organized in 2011, the SEA has attacked news agencies, government sites, universities, and other organizations deemed hostile to the Syrian government.
- In October 2013, the SEA hacked into a domain registry containing information about a number of different Qatari websites.
- The SEA pointed to Qatari support for the rebels in Syria as the reason for the attack.
- The SEA has, to date, focused on nuisance attacks, including placing pro-Assad propaganda on the Qatari websites or directing visitors to other sites.

Cover photo: Logo used by the [Syrian Electronic Army \(SEA\)](#).



# OEA Team Threat Report

## Map



*Figure 1: Map of Qatar*



# OEA Team Threat Report



---

## Introduction

The recent media attention given to the National Security Agency (NSA) domestically is putting more focus on cyber activities around the world. The NSA's more sophisticated operations have overshadowed the less complicated, but nonetheless effective, cyber attacks conducted by organizations such as the Syrian Electronic Army (SEA). Since its inception in 2011, the SEA has conducted nuisance attacks on numerous sites around the world in support of the Syrian government. News agencies, government sites, universities, and even the US Marine Corps recruiting site have been targets of the SEA's cyber attacks.

Most recently, the SEA targeted Qatari government ministry websites. The Qatari government gained control of the online sites within a few days, but the event underscored the ease with which cyber attacks can be waged from anywhere in the world. The SEA's reason for targeting Qatar is the country's support of the Free Syrian Army and affiliated Sunni insurgents fighting against the Assad government. The SEA has restrained itself to nuisance attacks and not malicious assaults; however, it is not unrealistic to posit more damaging attacks in the future. The ability to wage attacks from anywhere in the world and operate within disparate and disconnected cells allows cyber insurgents to conduct operations more easily than traditional insurgents.

---

## Syrian Electronic Army (SEA)

The SEA is a disparate group of computer hackers both inside and outside Syria who support the Assad government. The purported goal of the SEA is to counter what it perceives is unfair coverage of the Syrian government in the Western and Arabic press and support of governments for rebels fighting against the Syrian government. Operating online via social media platforms such as Facebook and Twitter, the SEA has launched organized nuisance attacks such as spamming campaigns and denial of service attacks on individual, group, and organization websites that it believes undermine the Syrian government's legitimacy.<sup>1</sup> The SEA Facebook page claims that it is not an official political party and is only associated with the Syrian government through its support of the government against an insurgency supported by other countries.<sup>2</sup>

Since 2011, the SEA has conducted what can be defined as nuisance attacks on numerous sites, but most organizations targeted regained control of their websites within a few hours to a few days. One self-described member of the SEA network stated that his intent was not to destroy, but to publish messages or articles of support for the Syrian government. A veiled threat, however, followed when the hacker said that if the United States attacked Syria, more malicious and damaging attacks could result.<sup>3</sup> The SEA has three years of successful experience probing a large number of websites. Its collective skills at that level are sharp, yet it is unlikely that the SEA will be able to progress much further into more complicated cyber attacks without significant help from allies. Those capable of higher-level technology attacks are not likely to share those resources with the SEA, as it would create vulnerability for the sharing entity.



## OEA Team Threat Report



The SEA is not a monolithic organization, but operates in a decentralized fashion, in a manner similar to insurgent cells. Loosely-aligned affiliations allow hackers to contribute to mutual goals, but without a hierarchical structure. On the SEA's now-defunct website, it listed a number of hackers who had an identity under the SEA's umbrella organization, but were able to operate independently. The website



**Figure 2: Now defunct SEA website calling for volunteers**

shown in Figure 2, recently taken down by its domain registering host, recruited anyone interested in furthering the Syrian government cause. The text in the upper left asked for volunteers in less than perfect prose:

“To contribute with us in supporting the cause of the Syrian Arab people by armaments with science and knowledge against the campaigns led by the Arab media and Western on our Republic by broadcasting fabricated news about what is happening in Syria. You can join our page via social networking sites: Facebook - Twitter or by publishing videos that display on our



# OEA Team Threat Report



page on You Tube. join to our pages by clicking on the links below to be one of the Syrian electronic."

In the lower left corner of Figure 2, SEA outlined the procedure for becoming an affiliate and the procedure for having an anonymous presence on the SEA website:

"You can now get a membership card in the Syrian Electronic Army by registering the data that you wish to be shown, you must register as a membership on the site first, it will express your electronic identity card and its data can't be modified without approval of management, to create your own card now Click Here."

## Syrian Electronic Army Cyber Attacks

This list of the SEA's attacks is not all inclusive, but provides a sense of the number and scope of their operations:

**July 2011: University of California Los Angeles** – website defaced by SEA hacker known as "The Pro"<sup>4</sup>

**September 2011: Harvard University** – homepage was replaced with an image of Syrian president Bashar al-Assad, with a message stating, "Syrian Electronic Army Were [sic] Here"<sup>5</sup>

**April 2012: LinkedIn** – took down the official blog site and redirected visitors to a site supporting Bashar al-Assad<sup>6</sup>

**August 2012: Reuters News Agency** – twenty-two Twitter account tweets were sent with false information on the conflict in Syria and a false report was posted to a Reuters journalist's blog on the news website<sup>7</sup>

**February 2013: Sky News Arabia** – pro-Syrian government comments were written on the main Twitter account @skynewsarabia, used for cultural and entertainment news, and its Facebook page, facebook/skynewsarabia<sup>8</sup>

**April 2013: Associated Press** – through Twitter account, falsely claimed the White House had been bombed and President Barack Obama was injured. The tweet was re-tweeted thousands of times within minutes and caused the Dow Jones Industrial Average index to drop sharply before quickly recovering<sup>9</sup>

**May 2013: The Onion** – Twitter account was hacked by phishing Google app accounts of The Onion's employees<sup>10</sup>

**May 2013: The ITV News London** – Twitter account was hacked.<sup>11</sup>



# OEA Team Threat Report



**May 2013: Sky News** – compromised several Sky News Android applications, requiring users to reload the apps.<sup>12</sup>

**July 2013: Truecaller** (a global phone directory application for smartphones and feature phones) – SEA claimed it hacked into servers and stole seven databases and released TrueCaller's database host ID, username, and password via a tweet. On 18 July 2013, Truecaller issued a statement on its blog stating that its servers were indeed hacked, but claiming that the attack did not disclose any passwords or credit card information.<sup>13</sup>

**October 2013: US President Barack Obama** – Twitter and Facebook accounts were hacked into, diverting site visitors to a Syrian propaganda video<sup>14</sup>

**July 2013: Viber** (proprietary cross-platform instant messaging voice-over-Internet protocol application for smartphones developed by Viber Media) – accessed two minor systems: a customer support panel and a support administration system; according to the company's official response, no sensitive user data was exposed and Viber's databases were not hacked<sup>15</sup>

**August 2013: Outbrain** (advertising service) – hacked via a spearphishing attack, allowing placement of redirects into the websites of The Washington Post, Time, and CNN<sup>16</sup>

**August 2013: NYTimes.com** – domain name registration (DNS) was hacked, causing redirection from the website to a page that displayed the message "Hacked by SEA;" Twitter's domain registrar was also changed<sup>17</sup>

**August 2013: Twitter** – DNS registration hacked to show the SEA as its admin and tech contacts<sup>18</sup>

**August 2013: The New York Times, Huffington Post, and Twitter** – took control of media website domains<sup>19</sup>

**September 2013: US Marine Corps Recruiting** – hacked into the Internet recruiting site for the US Marine Corps, posting a message that urged US Soldiers to refuse orders if Washington decides to launch a strike against the Syrian government<sup>20</sup>

**September 2013: Global Post** – targeted its official twitter account and website (globalpost.com). SEA officially announced the hack through its twitter account, stating: "Think twice before you publish untrusted informations [sic] about Syrian Electronic Army" and, "This time we hacked your website and your Twitter account, the next time you will start searching for new job"<sup>21</sup>

**October 2013: Qatar Government** – hacked the Qatari domains registry (registry.qa), impacting the .qa domain websites of Google, Vodafone, Facebook, al Jazeera, Qatar Telecom, Sheikha Mozah, Qatar





# OEA Team Threat Report



Ministry of Foreign Affairs, the Qatar government portal, the Emir's Palace, the Qatar Armed Forces, and the Qatar Ministry of the Interior

**October 2013: US President Barack Obama** – through at least one staff member's Gmail account, hacked Twitter and Facebook accounts, redirecting visitors to a graphic 24-minute propaganda video on YouTube (subsequently removed)

## The Qatar Attack

Domain registration is the process by which a company or individual can obtain a website domain, such as [www.yoursite.com](http://www.yoursite.com). The Internet Corporation for Assigned Names and Numbers (ICANN)\* manages the international Domain Name Server (DNS) database. ICANN ensures that all registered names are unique and map properly to a unique Internet Protocol (IP) address. The IP address is the numerical address of the website that tells other computers on the Internet where to find the server host and domain. Domain registration is available to the public via a registrar. Before a domain registration can be approved, the new name must be checked against existing names in the DNS database. Gaining access to the registrar's database allows a hacker, such as SEA, to alter the names of domains and gain access to websites. This is how SEA gained access to Qatari websites in October 2013.

There are a number of ways to gain access to an organization's website. Figure 3 below illustrates a simplified way in which SEA might have gained access to the Qatari domain registry, which gave it access to a number of websites. (A detailed consideration of hacking techniques and software is beyond the scope of this Threat Report.) Figure 3 also illustrates the vulnerability organizations face as they exist in a digital world, particularly with the readily available and free-flowing information on Internet social media sites.

A hacker first uses blogs, social network sites, websites, etc. to find email addresses of people within an organization. Using that information, the hacker sends an email to the address with a downloadable file, acting as a Trojan horse, that contains an embedded remote access tool (RAT). Once the email recipient is enticed to open the attached file, the RAT is activated and able to send password and other sensitive information back to the hacker. With the acquired information, the hacker can enter the domain registry. Once in the domain registry, the hacker can change domain names and modify websites.

---

\* ICANN is a non-profit corporation located in Marina Del Rey, California tasked with managing Internet Protocol (IP) addresses and domain names.





# OEA Team Threat Report

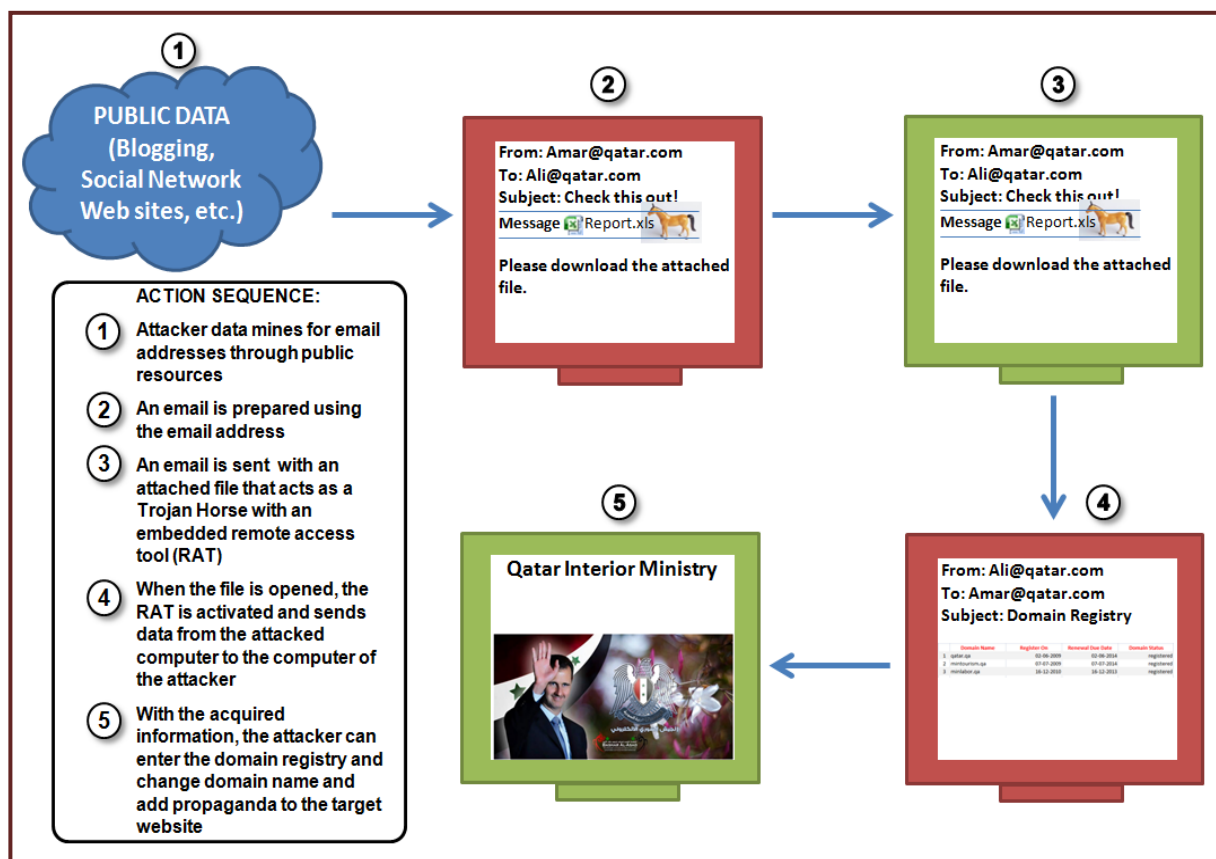


Figure 3: Cyber attack

## Analyst Assessment

The SEA is a loosely-aligned group of computer hackers intent on righting what they perceive to be unfair treatment of the Syrian regime by Western and Arab media and governments. It is currently capable of nuisance attacks on most Internet websites, including Facebook and Twitter. The SEA attacks have been successful due to the group's ability to exploit innate weaknesses in the security of Internet sites. Despite threats that it would be forced to resort to more damaging attacks if provoked by an attack by outside forces, there is no evidence the SEA could actually carry out such an attack without help from Syrian allies such as Russia, China, or Iran. It is highly unlikely that any of these countries would entrust any kind of more sophisticated tools or resources to the SEA.

Continuing successful nuisance attacks, however, will have an effect. Time lost in regaining control of a website and loss of customer confidence in the ability of an organization to protect sensitive data will have an economic impact. It is possible that the SEA has the capability to hack into systems that hold



# OEA Team Threat Report



credit card and other sensitive information. These kinds of criminal attacks have been successfully performed by other groups with devastating effects on consumer confidence. The SEA has only shown an interest in pressing a propaganda agenda to date, but shifts in policies or coverage might cause the SEA to up the digital ante.

There is no evidence, however, that these attacks are swaying anyone to the side of Syria. Indeed, there is evidence that continued attacks may complicate the SEA's cause. In the aftermath of an attack on the New York Times, the SEA's webpage was taken down by the Internet registrar hosting the site. One of the more bizarre and interesting results of the SEA's growing prominence is its challenge to one of the most notorious and infamous international hacker groups. In what resembled cyber gangs fighting over territory, Anonymous and the SEA faced off on opposing sides of the Syrian conflict beginning in 2011. Attacks have been accompanied by the tough talk typical of two gangs, each trying to one-up the other. In September 2013, the SEA denied claims by Anonymous that it had hacked into SEA's system.<sup>22</sup> The SEA is clearly a force of disruption, and the long-term implications of its continued presence might very well remain what they are today – primarily a nuisance – or the implications might become more serious if the SEA's message gains greater influence.

## Training Implications

- All Internet-based sites are vulnerable to cyber attacks.
- Information gained from social media and other Internet sites can be used to facilitate successful cyber attacks.
- Hackers are able to operate within disconnected organizations, each with similar goals and operating independently under a larger umbrella.
- All suspicious emails should be viewed as a threat.

## Related Products

Follow these links to view related products:

- [Syrian Social Media](#)
- [OE Quick Guide: Syria](#)
- [The Free Syrian Army-From Rifles to MANPADS](#)

See also the [Red Diamond Newsletter](#), which contains current articles on a variety of topics useful to both soldiers and civilians ranging from enemy TTP to the nature and analysis of various threat actors.

For detailed information on weapons and equipment, see the [Worldwide Equipment Guide](#).

To see more products from TRISA-CTID, visit the Army Training Network (ATN):

[https://atn.army.mil/dsp\\_template.aspx?dpID=377](https://atn.army.mil/dsp_template.aspx?dpID=377)



# OEA Team Threat Report



**ATN**  
Army Training Network  
Training Solutions to Stay Army Strong

myFavorites Home Unit Training Management myTraining Videos Products Links Collaborate Print

Home >> CTID Operational Environment Page

**CTID Operational Environment Page**

**Purpose:** CTID is the Army's lead to study, design, document, validate and apply Hybrid Threat and Operational Environment (OE) conditions that support all U.S. Army and joint training and leader development programs.

**TRISA Handbooks:**  
[Irregular U.S. Army TRADOC Forces Handbook No. 1.08](#)  
[Insider Threat September 2012](#)  
[FOUO AWG Subterranean Warfare Handbook](#)  
[Irregular Forces Financing Handbook March 2012](#)  
[Other Handbooks Produced by CTID \(FOUO\)](#)

**Operational Environment Products** - A listing of reports, handbooks, and guides, describing the operational Environment training and exercise design purposes.

<a href="#">Decisive Action Training Environment</a>	<a href="#">OE Estimate</a>
<a href="#">Regionally Aligned Forces Training Environment (RAFTE) Africa</a>	<a href="#">Operational Environment Assessments</a>
<a href="#">OE Quick Guides</a>	<a href="#">Terrorism Handbooks</a>
<a href="#">Red Diamond Newsletters</a>	<a href="#">Threat Reports</a>
<a href="#">Threat Assessments</a>	

[Threat Force Structure Page](#)

[Hybrid Threat Train the Trainer Course](#)

and Army Knowledge Online (AKO): <https://www.us.army.mil/suite/portal/index.jsp>

**Threat Products: AKO "Easy-Link"**  
Contemporary Operational Environment and Threat Integration Directorate

1. Login  
2. "Click" Files  
3. Search to:  
TRADOC G2  
TRISA-CTID  
4. "Click" & Find !



# OEA Team Threat Report



---

## POCs

---

OEA Team  
913-684-7929 (COMM)  
552-7929 (DSN)

TRADOC G-2 Intelligence Support Activity (TRISA)  
Complex Operational Environment and Threat Integration Directorate (CTID)  
803 Harrison Drive, BLDG 467  
Fort Leavenworth, KS 66027

---

## Figure Credits

---

Figure 1. [Map of Qatar](#). CIA World Factbook, 31 October 2013.

Figure 2. Now defunct SEA website calling for volunteers.

Figure 3. Cyber Attack. TRISA.

---

## End Notes

---

<sup>1</sup> Sarah Fowler, "[Who is the Syrian Electronic Army](#)," BBC News Middle East, 25 April 2013.

<sup>2</sup> "Syrian Electronic Army," Facebook, 31 October 2013.

<sup>3</sup> Byron Acohido, "[Syria's Cyber Retaliation Signals New Era of Warfare](#)," USA Today, 30 August 2013.

<sup>4</sup> Bruce Sterling, "[Syrian Electronic Army Invades University of California Los Angeles](#)," Wired, 6 July 2011.

<sup>5</sup> Sean Coughlan, "[Harvard Website Hacked by Syria Protesters](#)," BBC News Education & Family, 26 September 2011.

<sup>6</sup> Kris Holt, "[Syrian Hackers Take Down LinkedIn's Official Blog](#)," The Daily Dot, 26 April 2012.

<sup>7</sup> "[Reuters Twitter Account Hacked, False Tweets about Syria Sent](#)," Reuters, 5 August 2012.

<sup>8</sup> "[Sky News Arabia Twitter and Facebook Accounts Hacked by Syrian Electronic Army](#)," Softpedia, 7 February 2013.

<sup>9</sup> Gerry Smith, "[Syrian Electronic Army's AP Hack Just the Latest Phishing Attack on a Major News Organization](#)," Huff Post Tech, 23 April 2013.

<sup>10</sup> "[How the Syrian Electronic Army Hacked the Onion](#)," Onion Inc.'s Tech Blog, 8 May 2013.

<sup>11</sup> Sabari Selvan, "[ITV News London Twitter Account Hacked by Syrian Electronic Army](#)," E Hacking News, 24 May 2013.

<sup>12</sup> "[Syrian Electronic Army Compromises Sky Android Apps](#)," ITV, 26 May 2013.

<sup>13</sup> Sabari Selvan, "[Truecaller Database hacked by Syrian Electronic Army](#)," E Hacking News, 17 July 2013; "[TrueCaller hacked, 1 million Indians' data at risk](#)," The Times of India, 18 July 2013; "[Truecaller Statement](#)," True Software Scandinavia AB, 18 July 2013.

<sup>14</sup> Amanda Paulson, "[Syrian Electronic Army Says it Hacked Obama Accounts](#)," DC Decoder, 29 October 2013.

<sup>15</sup> Jordan Crook, "[Viber Attacked by Syrian Electronic Army](#)," Tech Crunch, 23 July 2013.

<sup>16</sup> Philip Bump, "[Syrian Hackers Use Outbrain to Target The Washington Post, Time, and CNN](#)," The Atlantic Wire, 15 August 2013.



# OEA Team Threat Report



- 
- <sup>17</sup> Suzanne Choney, "[New York Times hacked, Syrian Electronic Army suspected](#)," NBC News, retrieved 28 August 2013.
- <sup>18</sup> Mario Aguilar, "[Syrian Electronic Army Claims It's Taken Over Twitter's Domain \(Updated\)](#)". Gizmodo, 27 August 2013.
- <sup>19</sup> Steve Kovach, "[Syrian Electronic Army Suspected in Web Attack on New York Times, Twitter, and Huffington Post](#)," Business Insider, 27 August 2013.
- <sup>20</sup> Julian Barnes, "[Syrian Electronic Army Hacks Marines Website](#)," The Wall Street Journal, 2 September 2013.
- <sup>21</sup> "[GlobalPost hacked by the Syrian Electronic Army](#)," GlobalPost, 30 September 2013.
- <sup>22</sup> Hunter Stuart, "[Syrian Electronic Army Denies Being Attacked by Anonymous](#)," Huff Post Tech, 4 September 2013.