

Syria and propaganda warfare: the Syrian Electronic Army¹

“Consumerization of warfare”, a concept coined by Andrea Zapparoli Manzoni, has been identified by the website *Hackmageddon.com* as one of the crucial aspects of new warfare.² Paolo Passeri writes: “If the Cyberspace is the fifth domain of war, social media are likely destined to become the major sub-domain.”³

Consumerization of warfare has been defined by Zapparoli Manzoni and Passeri as the growing use of new technology such as social media and mobile⁴ in a new war format, especially for propaganda.⁵ The authors state:

“The issue is considerably more complicated than a simple tweet or a Facebook status update (a method that, although unconfirmed, is said to have been used by the Syrian Government to distribute DDoS software to its supporters for attacking adversary sites), and hides the (usual and well known) Social Network security issues, which are projected in a military dimension extending them in a much larger and dangerous scale both for senders and recipients of the tweets.

The main security concern relies in reputation, a blessing and a curse for Social Networks.”⁶

The Syrian case mentioned above is a striking example illustrating this new kind of warfare. But the use of computer mediated communication is not a new phenomenon for the Middle East. In October 2000 Israeli hackers successfully hacked several websites of the Lebanese Hizbullah and started what has been called by the media a “Cyber Intifada” since Lebanese and Palestinian hackers started to retaliate by attacking and esp. defacing Israeli websites. This campaign was the first instance of governmental and non governmental propaganda warfare in the region.⁷ The Iranian activities against the protesters of the “Green Movement” after the presidential elections of 2009 are well known. An Iranian hacker group, the *arteš-e sāybarī* (Iranian Cyber Army)⁸, is known for attacks on *Baidu* or *Twitter*.⁹ Its creation was first proposed in 2005 by the Revolutionary Guards.

1 This article is a slightly revised version of the article “Syria and electronic warfare”.

2 Zapparoli Manzoni/Passeri 2011

3 Passeri 2011a

4 Passeri 2011b

5 Zapparoli Manzoni/Passeri 2011

6 Zapparoli Manzoni/Passeri 2011

7 Cf. Kirchner 2003.

8 There are other groups operating or advertising themselves on the Web, e.g., the “Cyber Army of Jerusalem” (*sepāh-e sāybarī-ye Qods*) (<http://scqods.blogfa.com/>) (accessed 03/22/2013).

9 <http://cyber-army.blogfa.com/> and http://fa.wikipedia.org/wiki/ارتش_سایبری_جمهوری_اسلامی_ایران and <https://csis.org/blog/iranian-cyber-army> (accessed 03/22/2013)

An organization called Iranian Cyber Army is active on Facebook.¹⁰ Other hacker groups were operating before.¹¹ The “Iranian Cyber Army” changed from defacements to establishing botnets in 2010.¹² Another important field of pro-government activities is Bahrain.¹³ A group called *Algerian Cyber Army* is active on Facebook with a mixed assortment of postings.¹⁴ Other *cyber armies* from outside the region are active in the Middle East, too.¹⁵

Syrian Electronic Army

The Syrian situation is characterized by Gonzalez-Quijano as a “regime of truth”¹⁶ trying to use the Web as a means of control – e. g., opening up Web services to allow a survey of online activities of anti-regime activists – and of propagating its own truth, attacking other online sites suspected to offer “wrong” information.¹⁷

One of the most active groups is the Syrian Electronic Army, famous *inter alia* for its attack on the AP Twitter account:

“Remember that day when the Associated Press Twittter account said "Breaking: Two Explosions in the White House and Barack Obama is injured"? Remember feeling like the world was ending? Never mind that the style (AP has a distinct style found in its rulebooks) and syntax wasn't what AP normally used, and AP normally uses SocialFlow but this one was posted from the web.

But within minutes it was retweeted 4,000 times. The stock market certainly had the Chicken Little mindset... the Dow Jones had a huge, huge drop.

But later on April 23, 2013 the Twitter account was suspended, and the AP CorpComm account revealed that the doomsday tweet was all a hoax, perpetrated by a bunch of ornery computer-gifted Syrians who like the Syrian dictator Bashar al-Assad perhaps too much. The stock market promptly recovered upon learning of this revelation.”¹⁸

10 <https://www.facebook.com/pages/%D8%A7%D8%B1%D8%AA%D8%B4-%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86-Iranian-Cyber-Army/153687871449800> (accessed 11/22/2013).

11 <http://en.irangreenvoice.com/article/2010/feb/19/1236> (accessed 03/22/2013); there are incidents hinting at a use of the label “Cyber Army” for low level hacking, e.g., the recent hack of a German school website (<http://cyberwarzone.com/iranian-cyber-%E2%80%8B%E2%80%8Barmy-hacked-porsche-school>) (accessed 03/22/2013).

12 <http://www.zdnet.com/blog/security/iranian-cyber-army-building-botnet-with-exploit-kit/7561> (accessed 03/22/2013).

13 Yorks 2011.

14 <https://www.facebook.com/AlgeriaCyberArmy> (accessed /11/22/2013).

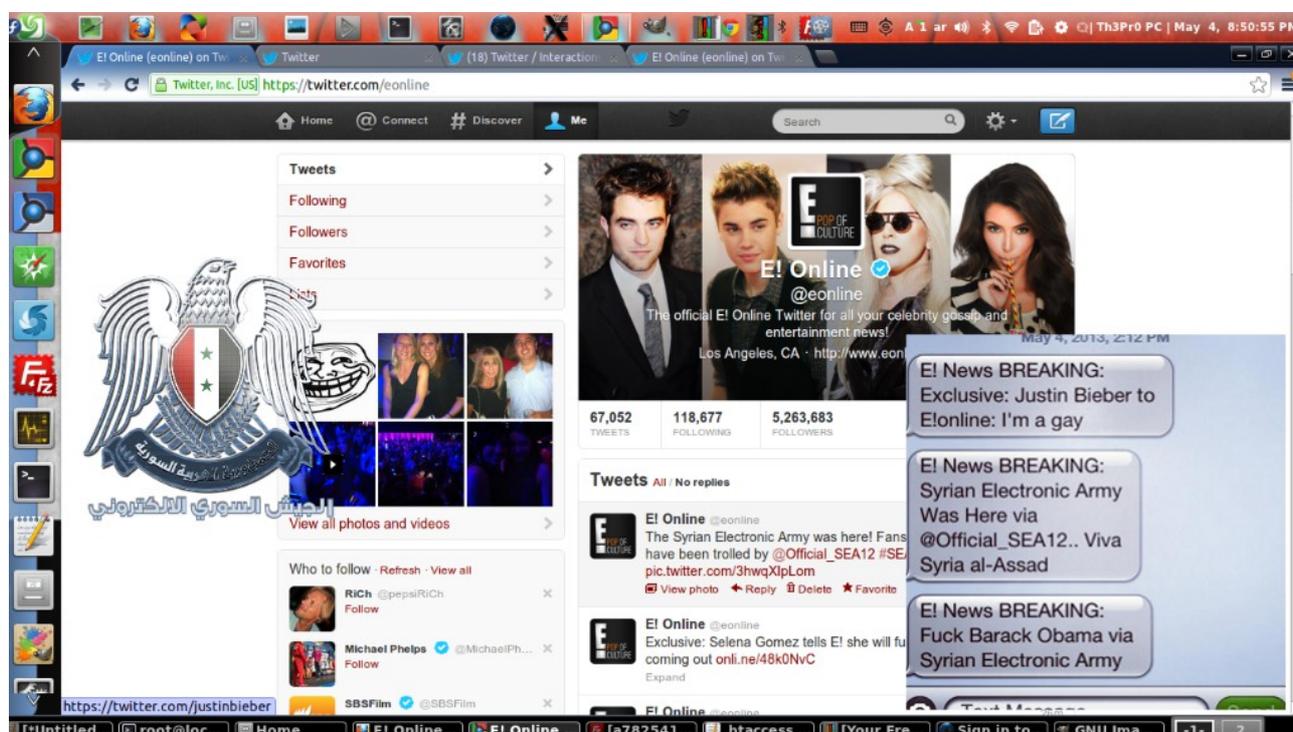
15 A *Portugal Cyber Army* attacked Dubai International Airport in April 2013 (<http://www.ehackingnews.com/2013/04/dubai-airport-site-hacked.html>) (accessed 04/20/2013).

16 Gonzalez-Quijano 2012, p.136.

17 An overview in Gonzalez-Quijano 2012, p.136ff., Lohlker/Telič 2013.

18 http://ohinternet.com/Syrian_Electronic_Army (accessed 05/05/2013).

Effective on another level may be the attack on the Twitter account of *E! Online* tweeting a fake headline about teenie idol Justin Bieber.¹⁹ The first tweet 'reveals' Bieber to be gay, a subtle hint at the mindset of the SEA people – even if it should be regarded as a successful attempt to get attention to the following tweets²⁰:



Who are these hackers? “We do care about what is happening to our country”, Voice of Russia was told by a member of Syria's Electronic Army.²¹ The Syrian Electronic Army (*al-jaysh al-iliktruniyy as-suriyy*) is one of the most active groups in Southwest Asia targeting cyberspace.²² A thorough analysis of the Syrian Electronic Army is still necessary.²³

The group is presenting itself as an independent initiative of Syrian patriots. Since the group was inspired by the Syrian Computer Society – the current president Bashar al-Assad was president of the society before assuming presidency²⁴ – and was hosted on the server of this society the intimate relations to the regime²⁵ is evident.²⁶ The more, the group was hailed publicly by president Bashar al-Assad.

19 <http://www.brianbrown.net/2013/05/04/syrian-hackers-take-over-e-online-twitter-tweet-fake-headline-about-justin-bieber-2/> (accessed 05/05/2013).

20 The screenshot is copied from <http://sea.sy/article.php?id=1955&lang=ar> (accessed 05/05/2013).

21 http://english.ruvr.ru/2013_02_01/Syria-s-Electronic-Army-We-care-about-our-country/ (accessed 03/08/2013).

22 The foremost ally of Syria, the Islamic Republic of Iran, boasted in 2013 to have "the fourth biggest cyber power among the world's cyber armies" as part of the revolutionary guards (<http://english.farsnews.com/newstext.php?nn=9107141074>) (accessed 03/08/2013).

23 Preliminary results of current research are available in Rüdiger Lohlker/Anna Telič. Die Rolle von »Social Media« in der syrischen Revolution, in Fritz Edlinger/Tyma Kraitt (eds.), *Syrien: Hintergründe, Analysen, Berichte*, Vienna: Promedia 2013, pp.175-187. A first comprehensive article on the SEA was published on <http://www.infowar-monitor.net/2011/05/7349/> (accessed 03/22/2013).

24 The society was founded

25 To be understood as the complex of institutions supporting the government and ruling elite.

26 Lohlker/Telič 2013, p.184

But in May 2013 the SEA announced that the Syrian Computer Society stopped hosting the website of the SEA.²⁷ This is the second time the Syrian Electronic Army lost his home in 2013, since a U.S. firm in observation of international trade sanctions against Syria “has seized hundreds of domains belonging to various Syrian entities”²⁸, amongst them the SEA. But the new homepage of the Syrian Electronic Army is still hosted in Damascus. A who is-research (November 22, 2013) yields the following results:

Domain Name: sea.sy
IP: 141.105.64.37
Owner Name: Syrian Electronic Army
Address: Syria
Damascus, Damas
10001
Syria

We may assume a formal distance from the Syrian Computer Society and the regime, but not a substantial change of the intimate relation to the regime.

Before being relocated to a Syrian domain, the SEA was also hosted in Moscow at a company called *Shorefront Media*.²⁹

The former Whois-entry for its IP address 213.178.227.152 in 2011 read quite clear that the ISP is “SCS-Net, ISP based in Damascus, Syria”.³⁰

“The following is the Army’s domain name registration record as retrieved from domain name WHOIS database:

syrian-es.com
Registrant:
NET, SCS-
Beirut Street
Damascus, SY 13365
SY
Domain Name: SYRIAN-ES.COM
Administrative Contact , Technical Contact :
NET, SCS-
domreg@scs-net.org
Beirut Street

27 http://www.salon.com/2013/05/31/syria_takes_down_syrian_electronic_army_partner/ (accessed 11/22/2013).

28 <https://krebsonsecurity.com/2013/05/trade-sanctions-cited-in-hundreds-of-syrian-domain-seizures/> (accessed 11/22/2013).

29 <http://krebsonsecurity.com/wp-content/uploads/2013/08/dt-141-sea.png> (accessed 11/22/2013).

30 Accessed 03/22/2013.

Damascus, SY 13365
SY
Phone: +96311446677636
Record expires on 05-May-2012
Record created on 05-May-2011
Database last updated on 05-May-2011
Domain servers in listed order:
NS1.SCS-NET.ORG 213.178.225.4
NS2.SCS-NET.ORG 213.178.225.3”³¹

A back-up domain *syrianelectronicarmy.com*, IP address 213.178.227.152, has been registered on February 24, 2013 showing the following server data:

IP location: Dimashq – Damascus – Syrian Computer Society Scs

ASN: AS29256 INT-PDN-STE-AS Syrian Telecommunications Establishment

Three domains are hosted at IP address 213.178.227.152: *syrian-es.com*, *syrian-es.net*, and *syrianelectronicarmy.com*, an evident connection to the former domain as shown by the meta description hinting at *syrian-es.org*.³²

The URL of the SEA homepage in May 2013 was (and still is) <http://www.sea.sy>. Rumours at that time, the SEA may have been transferred to Dubai, seem to have been premature.³³

Helmi Noman writes in a first overview:

“The Syrian Electronic Army, also known as Syrian Electronic Soldiers, claimed on its “about” web page when it was launched in the second week of May 2011 that it was not an official entity, but rather a group of young people who love their country and have decided to fight back electronically against those who have attacked Syrian websites and those who are hostile to Syria. The Army replaced its “about” web page with a new one on May 27, 2011. The Army removed from the new page the reference to it not being an official entity and said it was founded by a team of young Syrian enthusiasts to fight those who use the Internet and especially Facebook to “spread hatred” and “destabilize the security” in Syria. References to it not being an official entity were still found on other pages on the site as footnotes.”³⁴

Defacements – an important field of operation for the SEA – have been done by the handle “ArabAttack”; other handles used were “The Shadow”, “The Pr0” (see below), “SaQeR,SyRia”,

31 Noman 2011

32 All data <http://whois.domaintools.com/syrianelectronicarmy.com> (accessed 04/13/2013)

33 <http://www.guardian.co.uk/technology/2013/apr/29/hacking-guardian-syria-background> (accessed 05/05/2013).

34 Noman 2011.

“Sy Team”, and “al3arab”³⁵, another one is SyRiAn Cyb3r Army.³⁶

Some of the operations of SEA on Facebook show a similarity to networks like *Koobface*³⁷, “an evil doppelgänger”³⁸ of Facebook, stated Max Fisher and Jared Keller in one of the first articles on the SEA, published in *The Atlantic* August 31, 2011.³⁹ Their assessment of the SEA :

“Whoever they are, they've led by far the most sophisticated and highly visible online pro-regime effort of the 2011 Arab uprisings. Both Egypt and Libya tried shutting down Internet access outright, extreme steps that slowed communication but failed to stop the more tech-savvy activists from using proxies and special dial-ups to communicate (the blackout also had the unintended effect of angering otherwise uninvolved bystanders). The Syrian Electronic Army shows a surprising ability to move within the same online spaces typically dominated by young activists. Though Tunisians and Egyptians were able to outmaneuver their governments in large part using social media, Syrian activists have not enjoyed the same monopoly over the Web. Syria's government, by treating the Internet as another battleground in the fight for control rather than simply as a set of tools and websites to be disabled, may be the first in the Arab world to understand the potential utility of counter-revolutionary organizing online.

The Syrian Electronic Army is notable for its targets, which are Syrian and non-Syrian alike. Their campaign does not seem too much distinguish between opposition organizers within Syria and sympathetic groups or media outlets outside of it. The digital war isn't just against fellow Syrians, and it doesn't respect national borders. Whether the tools it uses are misdirection, annoyance, or outright attack, it has not hesitated in expanding its focus outside of Syria.”⁴⁰

Who is visiting the homepage of the SEA? The audience geography at alexa.com tells us⁴¹: 25% from Syria, 11.8% from the United Kingdom, 11.2% from Saudi-Arabia, 9.6% from India, 2.1% from Algeria, and 1.8% from Turkey.

35 Information Warfare Monitor 2011

36 http://www.youtube.com/watch?v=cbbz7C_9z6U&list=UUa0rxhyewu7ER_yLq9dIRWA (accessed 05/05/2013) uploaded by *thepro112233*.

37 Villeneuve 2010.

38 Villeneuve 2010, p.I.

39 Max Fischer/Jared Keller, *Syria's Digital Counter-Revolutionaries*, August 31, 2011

(<http://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/>) (accessed 03/23/2013).

40 Fisher/Keller 2011.

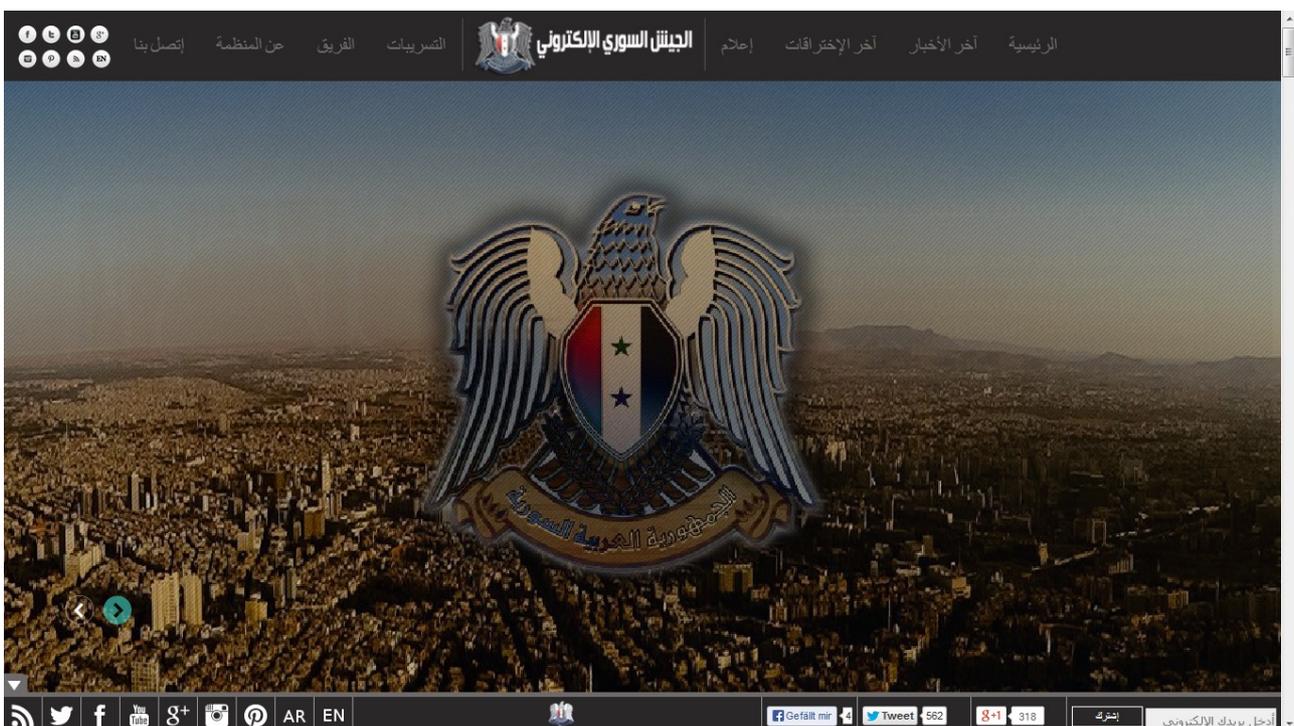
41 <http://www.alexa.com/siteinfo/sea.sy> (accessed 11/22/2013).

Homepage SEA

The central site of the web of the SEA is its “Official Web Site”:

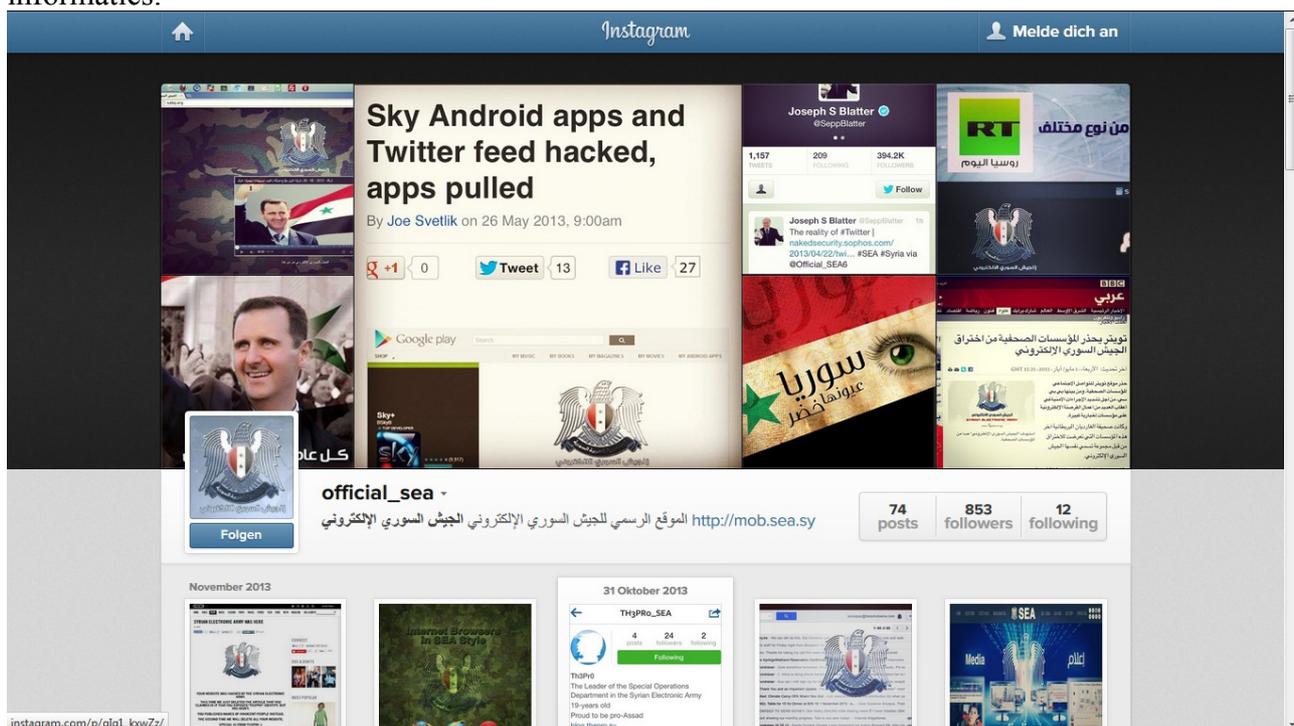


The new homepage has been slightly changed, but the logo and other elements are the same as before:



The site (Arabic-English) offers informations about the network around SEA with sites at Pinterest (<http://www.pinterest.com/officialsea/>), Instagram (http://instagram.com/official_sea/#), Google+ (<https://plus.google.com/+SeaSy/posts>), YouTube (<https://www.youtube.com/SEAOfficialChannel>), Facebook (<https://www.facebook.com/SEA.P.251>)⁴², and Twitter (https://twitter.com/Official_SEA 16). A RSS-feed is available.

As most important activists are mentioned⁴³: *VictOr* (see below), described as the main programmer and designer of all sites of the SEA, and *The Soul* (arab. *Dhā sūl*), described as responsible for the Facebook site of the SEA. Followed by *The Shadow*, a hacker, *Th3 Pr0*, leader of the special operations department, *Ism makhfiyy* (Anonymous), responsible for the social networking sites Twitter, Instagram, and Pinterest, *Ism makhfiyy* (Anonymous), responsible for the YouTube account, *Nasr Suriyya* (Eagle of Syria), responsible for the official e-mail account, *al-Mulhima* (The Inspiration), female member, responsible for graphics and design, and two other anonymous members, described as co-founders of the SEA. In story in the Syrian newspaper *al-Thawra* founding members of the Syrian Electronic Army were interviewed and identified as students of informatics.⁴⁴



The homepage offers recent news and recent hacks of the SEA. The reports of non-Syrian media about the operations of the SEA are documented. The team of the Syrian Electronic Army presents itself. A section on *Leaks* (see below) shows the documents retrieved from hacked Qatari, Turkish resources. A contact form is provided in case you want an official answer from the SEA.

42 Joined Facebook on November 22, 2013; 686 likes in three hours.

43 <http://sea.sy/index/ar> (accessed 11/22/2013).

44 http://thawra.alwehda.gov.sy/_print_veiw.asp?FileName=18216445320110516105347 (accessed 11/22/2013).

It is the main resource other SEA sites are referring to. An interesting fact is that the programs section disappeared.

The current (November 2013) Facebook group is no. 256, in May 2013 it was no. 206⁴⁵. It took six months to have 50 versions of the Facebook site, an indication for the ongoing battle for a Facebook presence. The current site sports a general statement pasted from version no. 251, acclamations by some users, The posts offered on No. 206 were on attacks by the SEA, remembering the good old days of Hafiz al-Assad, the former president of Syria, propagating strength and steadfastness⁴⁶ and e. g., a wording for future attacks.

The pictures at the Facebook pages of people posting on the Facebook wall of the SEA give interesting insights into the imaginary prevailing among regime supporters:



46 A number of comments stress the need to be steadfast.

Australian Syrian Electronic Army

The Syrian Electronic Army's efforts tried to be more diversified by creating several Facebook outlets. On June 27, 2011 the *Australian 4th Brigade Syrian Electronic Army* was created on Facebook.⁴⁷ This group presented itself as an initiative of “proud Syrians of Australia” supporting Bashar al-Assad as the “leader of the new democratic middle east”.⁴⁸

The *4th Brigade* shared some videos, some links, photos of Bashar al-Assad etc. One interesting photo is a still from a video showing today's Turkish PM Erdogan in 1990 sitting on the floor besides Gulbuddin Hekmatyar, founder of the Afghan Hezb-e Islami, and one of the main important Mujahidin leaders in the war against the Soviet Red Army. The comment links Hekmatyar to al-Qaeda – and through this link Erdogan to al-Qaeda. Reading the post at the video sharing website LiveLeak publishing this video we read a slightly more correct version telling us Hekmatyar founded the Hezb-e Islami, but telling Erdogan was educated by al-Qaeda and Taliban leaders, member of the Muslim Brotherhood, an organization founded by the British MI6, quoting his adversary on the Turkish Islamic scene, Erbakan, Erdogan and others are “tools in the hand of Zionism”, closing: “No need to tell you who created Al Qaeda in the first place.”⁴⁹ A fine piece of conspiratory thinking, slightly shortened by the *4th Brigade*.

The groups activity expired in December 2011, a very short-lived attempt to open a frontier far from the Middle East. Other Facebook groups still actively support the Syrian regime and its allies: one group the *Australian Syrians in Support of Bashar Al Assad* has a posting supporting the Facebook group *Electronic Resistance*, a Hizbullah outlet, against closure by Facebook.⁵⁰

The Pro Battalion

The most active of the online sites of *Th3 Pr0*, the alias used in interviews and one of the most active avatars of the SEA, was the Facebook group *The Pro Battalion*⁵¹, with a non-active blog and a newsfeed. The group joined Facebook in June 2012 and got up to 1549 likes (May 2013). The posts are sometimes to be found on the *Vict0r Battalion* site, too (see below). The illustrations are sometimes surprising, suggesting a quite apocalyptic mindset:

47 http://www.facebook.com/pages/Australian-4th-Brigade-Syrian-Electronic-Army/227398107281720#_=_ (accessed 03/08/2013).

48 Postings on 06/27/2011.

49 http://www.liveleak.com/view?i=218_1362051424 (accessed 03/09/2013).

50 <https://www.facebook.com/groups/152087361522897/> (accessed 11/22/2013).

51 <https://www.facebook.com/Th3Pr0.Official> (accessed 05/05/2013).



Vict0r Battalion – Syrian Electronic Army

Vict0r, the alias of one of the main activists (see below), started his own Facebook site in February 2013⁵², disseminating news about recent hacks of the SEA and propagating support for the regime of Bashar al-Assad:



The group got 2.532 likes and was still active in May 2013. In November the group changed to *Vict0r Battalion – Syrian Electronic Army*⁵³ with 600 likes, joined Facebook in September 2013. The new group posts pictures supporting Bashar al-Assad, the Syrian army, and the SEA, e. g., browser themes in SEA style:

⁵² <https://www.facebook.com/SEA.Vict0r.2> (accessed 05/05/2013).

⁵³ <https://www.facebook.com/SEA.Vict0r.3?fref=ts> (accessed 11/22/2013).



Twitter

Jillian C. York mentioned early pro-government activities at Twitter as early as October 2011. She wrote

“most trolls appeared to be automated feeds targeting the #Syria hashtag in an attempt to flood it, not with misinformation, but with irrelevant information. Though some individuals, such as myself, were targeted directly (and with my own Flickr photos of Syria, no less), Twitter’s infrastructure makes it relatively easy to block and report accounts for spam, and while many remained up, most were removed from search, making it easier for those using the #Syria hashtag to follow events on the platform.”⁵⁴

Not only the #Syria hashtag was flooded, #OpSyria was targeted, too. E. g., faked *Anonymous* videos are announced combining some symbols of *Anonymous* with Syrian counter-propaganda on the issue of chemical weapons.⁵⁵ The last sentences of the videos are quite clear: "May God protect Syria. its army. its leadership. and people". The comments of SEA supporters at YouTube were enthusiastic:

[Ninos Mussa](#)

SEA HAS WON! FUCK ANONYMOUS

54 Yorks 2011.

55 <http://www.youtube.com/watch?v=IyxII2kLKsc&feature=youtu.be> (accessed 04/05/2013).

SEA itself has an “official” Twitter profile, announcing 11529 followers and 17348 tweets (April 13, 2013). Most of the tweets are connecting to other files. Some examples:

Igor Rasputin @Mario__Savio [3h](#)

4/11/13 #Soros PsyOp #DemocracyNow's Amy uses bogus #HRW report <http://tinyurl.com/chryvnx> to attack #Syria
@Official_SEA @psych0r @GetOutNato
Retweetet von SyrianElectronicArmy

SyrianElectronicArmy @Official_SEA [12 Apr](#)

النطاق الاحتيالي لموقع الجيش السوري الإلكتروني | <http://www.syrianelectronicarmy.com/index.php> #سوريا

SEA Website Feed @SEA_Website [12 Apr](#)

<http://dlvr.it/3D4Rqj> الصفحة رقم 204 للجيش السوري الإلكتروني

Retweetet von SyrianElectronicArmy

“Twitter's security team appears playing whack-a-mole” with the SEA. “Twitter appears to have decided to put a stop to the Syrian Electronic Army's Twitter account [...] Sure enough, @Official_SEA has now been suspended.

How did the Syrian Electronic Army respond to their Twitter suspension? Well, they created a new account called @SyrianCyberArmy.

And when that one was shut down, they created yet-another-Twitter-account - @SEA_Official3.

Guess what? Yep, that one has been shut down too. And - as certain as night follows day - the SEA responded by creating @Official_SEA5.

You can probably guess what happens next in this story. That's right, @Official_SEA5 was suspended by Twitter.

Not that that has stopped the hackers, of course.

Currently, the Syrian Electronic Army are running a Twitter account at @Official_SEA6 - but you have to wonder how long before that one is also shut down by Twitter's security team.”⁵⁶

We are up to @Official_SEA16 now... The current Twitter account may be described as a hub distributing links to reports on operations of the SEA.

Other SEA related handles like *Vict0r* own their separate Twitter accounts.⁵⁷

56 <http://nakedsecurity.sophos.com/2013/04/22/twitter-syrian-electronic-army/> (accessed 11/22/2013).

57 <https://twitter.com/Vict0rSEA> (accessed 11/22/2013).

Hacks

The activities of the SEA focus at hacking websites and placing pro-government opinions, pictures etc. as pro-Assad counter-propaganda.⁵⁸ The leader of the “Special Operations Department” of the SEA claiming a number of SEA hacks, writes about himself at his blog (<http://blog.thepro.sy/>) using his nickname *Th3Pr0*, that he is 19 years old⁵⁹ and calls himself a programmer and hacker:



His most recent “achievement” include a hack of the blogs of *Channel 4*, hacks of Qatari websites (see below) and the US Marine Corps site trying to convince Marines that the Syrian army is fighting the same enemy: al-Qa’ida.⁶⁰ All his other hacks he claims personally are archived at *zone-h*⁶¹; the SEA has its own archive.⁶²

Recently some media outlets claimed to have revealed the identity of *Th3Pr0* and other members of the SEA. *Vice*, doing an interview with him before (see below), identified *Th3Pr0* as Hatem Deeb, a claim denied to *Vice* by *Th3Pr0*.⁶³ A little bit disturbing is the insistence on calling him the leader of the SEA while *Th3Pr0* claims to be the head of the special operations department... The debate about the identity of *Th3Pr0* produced a follow-up article by the security blo *Krebsonsecurity* referring to the article in the Syrian newspaper mentioned above.⁶⁴ The information he offers has to

58 For an overview cf. <https://recordedfuture.com/live/sc/kbIpWKW8fSF5> (accessed 05/05/2013).

59 His birthday must have been between April 2013 and November 2013.

60 <http://www.zone-h.org/mirror/id/20691009> (accessed 11/23/2013).

61 <http://www.zone-h.org/archive/notifier=The%20Pro> (accessed 04/20/2013).

62 <http://zone-h.org/archive/special=1/notifier=SEA> (accessed 04/20/2013).

63 <http://motherboard.vice.com/blog/is-this-19-year-old-the-leader-of-the-syrian-electronic-army> (accessed 11/22/2013).

64 For a second article v. <http://krebsonsecurity.com/2013/08/who-built-the-syrian-electronic-army/> (accessed 11/22/2013).

be looked at critically since he was not able to transcribe a part of the URL of the newspaper correctly, creating a Syrian journal *al-Wenda*, and ignoring the proper title of the newspaper.⁶⁵ His source *NBC News* at least had *al-Wehda*.⁶⁶

All this goes back to the server of the Syrian Electronic Army being claimed to be hacked and resources published. The Syrian Electronic Army reacted with scathing remarks at Twitter on August 31, 2013:

“@briankrebs Publishing fake screenshots and hacking randomly pro-Syria people unfortunately don't prove anything :)”⁶⁷

And *Vice* was hacked and the article on the presumed identity of *Th3 Pr0* deleted.⁶⁸

A few examples may give an impression of SEA's other activities:

The last website hacked at the time of writing this article was the site *anti-shabiha.com* operating against militia supporting the Asad-regime.⁶⁹ The site, claiming to be an intelligence site of the Free Syrian Army in Aleppo, published pictures and informations of people who are regarded as supporters of the regime.⁷⁰

In October 2013 the Qatar domain registry was hacked and various sites defaced⁷¹:

“Some major targeted websites belong to Al Jazeera, Vodafone, Google, Facebook, Sheikha Mozah, Qatar Ministry of Interior, Qatari Amir’s site, Qatar Exchange, Qatar Telecom, Qatari armed forces, Amir’s palace and Ministry of Foreign Affairs.”⁷²

In March 2013 three Twitter accounts of BBC were hacked for a short time: @bbcweather, @BBCarabicOnline, and @bbcradioulster. The purpose seemed to be deliver pro-Assad propaganda.

“Tweets included, “Saudi weather station down due to a head on-collision with camel”; “Tsunami alert for Haifa. Residents are advised to return to Poland.” One tweet alludes to UK financing for the rebels:

“Scandal: Edinburgh storm warning station decommissioned after maintenance fund diverted to arming

65 <http://krebsonsecurity.com/2013/08/syrian-electronic-army-denies-new-data-leaks/> (accessed 11/22/2013).

66 http://investigations.nbcnews.com/_news/2013/08/30/20250021-syrian-electronic-army-seen-as-nuisance-not-a-serious-cyberthreat (accessed 11/22/2013).

67 https://twitter.com/Official_SEA16/status/373883188734476288 (accessed 11/22/2013).

68 <http://hackread.com/vice-hacked-by-syrian-electronic-army/> (accessed 11/22/2013).

69 <http://www.zone-h.org/mirror/id/21205326> (accessed 11/23/2013); at the time of writing still offline, the Twitter account still works (<https://twitter.com/antishabiha>; accessed 11/23/2013).

70 <https://web.archive.org/web/20130808174905/http://www.anti-shabiha.com/> (accessed 11/22/2013).

71 For a list of the hacked sites v. <http://pastebin.com/67FPGbtR> (accessed 11/22/2013).

72 <http://hackread.com/sea-hacks-qatar-domain-registry/> (accessed 11/22/2013).

Syrian opposition.” Another alludes to Turkish support for the rebels: “Hazardous fog warning for North Syria: Erdogan orders terrorist to launch chemical weapons at civilian areas.”⁷³

The BBC hack was the reason *Vice* magazine tried to contact SEA and interviewed one member calling himself *Th3 Pr0*.⁷⁴ For the present text the most interesting information is the following answer:

“If FSA activists are planning on setting a bomb off or killing or kidnapping anyone, then yes, we'll tell the government. We don't hide the fact that many of the emails we obtained were forwarded to the Syrian government because of their importance and the fact they contained security and military information.”⁷⁵

Vice magazine conducted another interview with a member of *Anonymous* due to the exchanges of hacks by both groups, *Anonymous* supporting the Syrian opposition by an own operation like it had done in other Arab countries.⁷⁶ SEA liked at least the part of the article with the interview of its member, translating that part into Arabic.⁷⁷

On March 1, 2013, the Twitter account of the Qatar Foundation a government sponsored non-profit organization was hacked and messages sent out accusing Qatar to support terrorists.⁷⁸ One example:



Qatar Foundation @qatarfoundation

3 hrs

Need a new Career? #QatarFoundation will fund your training as a terrorist in #Syria pic.twitter.com/LrpfW8An2O

View photo

On April 25 2012 a Twitter account of a member of the Syrian Electronic Army posting from Utah⁷⁹ announced an attack on the social network *LinkedIn* accusing it to be used “to spread lies about Syria”.⁸⁰ Users were redirected to a page sporting the official Syrian flag, a picture of Bashar al-Assad in military gear and criticizing the Syrian National Council.⁸¹

Sometimes the sites hacked refuse to comment on attacks. On January 5, 2013, evidently the Payments Perspective Blog from Mastercard's Insights site was attacked adding “Hacked by Syrian

73 <http://www.infosecurity-magazine.com/view/31403/bbc-weathers-twitter-hacked-by-syrian-electronic-army/> (accessed 04/03/2013).

74 For another interview with *Th3Pr0* cf. <http://blog.thepro.sy/News/Content/Show/Node-ID/1868> (accessed 04/20/2013); *E Hacking News* was able to identify the interviewee.

75 http://www.vice.com/en_uk/read/the-syrian-electronic-army-hacked-the-bbc (accessed 04/05/2013).

76 *Vice* evidently did not check at least the online identity of the SEA representative they interviewed calling himself *Th3Pr0*. Otherwise they would have mentioned the blog of *Th3Pr0* (see above).

77 http://www.syrian-es.org/article.php?id=1931&utm_source=dlvr.it&utm_medium=twitter (accessed 04/05/2013)

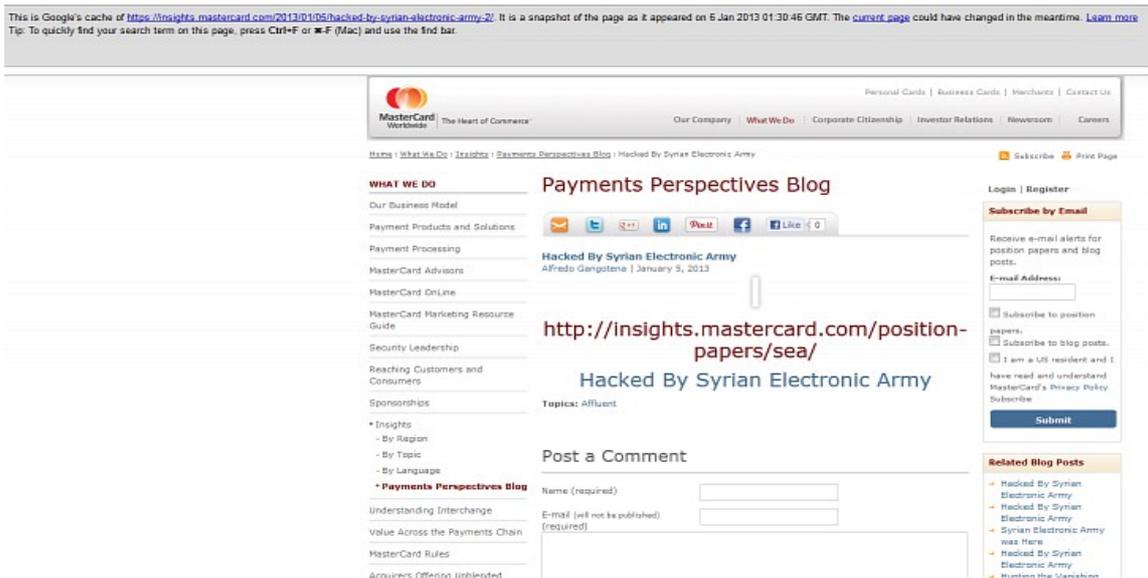
78 <http://qz.com/58274/syrian-electronic-armys-twitter-hacking-campaign-racks-up-another-victory/> (accessed 04/03/2013)

79 <http://thenextweb.com/me/2012/04/26/hackers-take-down-official-linkedin-blog-for-spreading-lies-about-syria/> (accessed 03/09/2013)

80 <http://www.siliconrepublic.com/strategy/item/26907-syrian-electronic-army/> (accessed 03/09/2013)

81 Ibid.

Electronic Army”⁸²



Human Rights online platforms are hacked. *Human Rights Watch* (HRW) Twitter feed was attacked on March 17, 2013:



This attack was hailed on a blog called *CounterPsyOps*⁸³: “Bravo to the Syrian Electronic Army!”⁸⁴ *CounterPsyOps* has an iconography demonstrating the bloggers' affinity to web and popular culture:



82 <http://news.softpedia.com/news/mastercard-blog-apparently-hacked-by-syrian-electronic-army-319866.shtml> (accessed 03/23/2013)

83 Bottom line: “A new hole in the propaganda matrix”.

84 <http://counterpsyops.com/tag/syrian-electronic-army/> (accessed 03/23/2013)

Title: Al-Assad against Western GCC Evil Forces



Title: Nato Wars



Anonymous vs. SEA – SEA vs. Anonymous

One of the most interesting moments was the showdown between SEA and Anonymous.⁸⁵ An interview with a member of the Anonymous campaign sheds light on this clash:

“Commander X is one of Anonymous' more vocal members and founder of the [People's Liberation Front](#) (PLF), a group linked with Anonymous who actively participating in **#OpSyria**, an anti-Syrian government hacking campaign, as well as other Arab Spring hacktivist operations. With all that in mind, I thought he'd be a good person to talk to.

VICE: Hi, Commander X. Can you tell me a bit about Anonymous' work in Syria and how you got involved with the conflict?"

Commander X: I and the PLF, under the flag of Anonymous, launched Operation Syria the very first week that the protests began in Deraa, Syria and the police had brutalised some young protesters [caught doing political graffiti](#) near the university there. As a movement, we were fresh out of victories in both Tunisia

⁸⁵ For an overview and examples of anti-Anonymous hacktivism see the McAfee white paper Paget 2012.

and Egypt, and I guess we felt that we and the Arab Spring were both sort of invincible. I think we all honestly felt Assad would be easy to topple – I don't think any of us back then could have predicted how things would turn out.

Our involvement in the events in Syria involve a sort of standard template within Anonymous and the movement that's come to be called "Freedom Ops". So our focus is, first and foremost, how do we keep the activists and protesters on the ground – as well as the entire population of Syria – safely connected to the internet? We also distribute the **Anonymous Care Package**, providing tech support for journalists and activists, media campaigns and, of course, offensive attacks on government web assets.

Can you tell me about your war with the Syrian Electronic Army?

The SEA was actually founded by Assad back when he was thought to have next to no chance of inheriting his fathers position as dictator because he was just such a geeky nerd. So they've been around a while, and we were aware from day one that they could become involved in the cyber conflict. As for our dealings with them, that's pretty straightforward. They are, by their own choice of allegiance to the dictator, the enemies of Anonymous. And they introduced themselves into the conflict fairly early on with a rather spectacular hack of a fairly well known Anonymous web site. We, in turn, responded by attacking their web assets and that conflict continues to this day.

It's a cyber war; they attack our assets, we attack theirs. They have their victories, and some spectacular defeats, and we have ours. To be honest, the war has gone on so long now you could probably fill up a book if you were to detail every engagement between Anonymous and the SEA.

Does Anonymous have a plan of action in place to target the SEA?

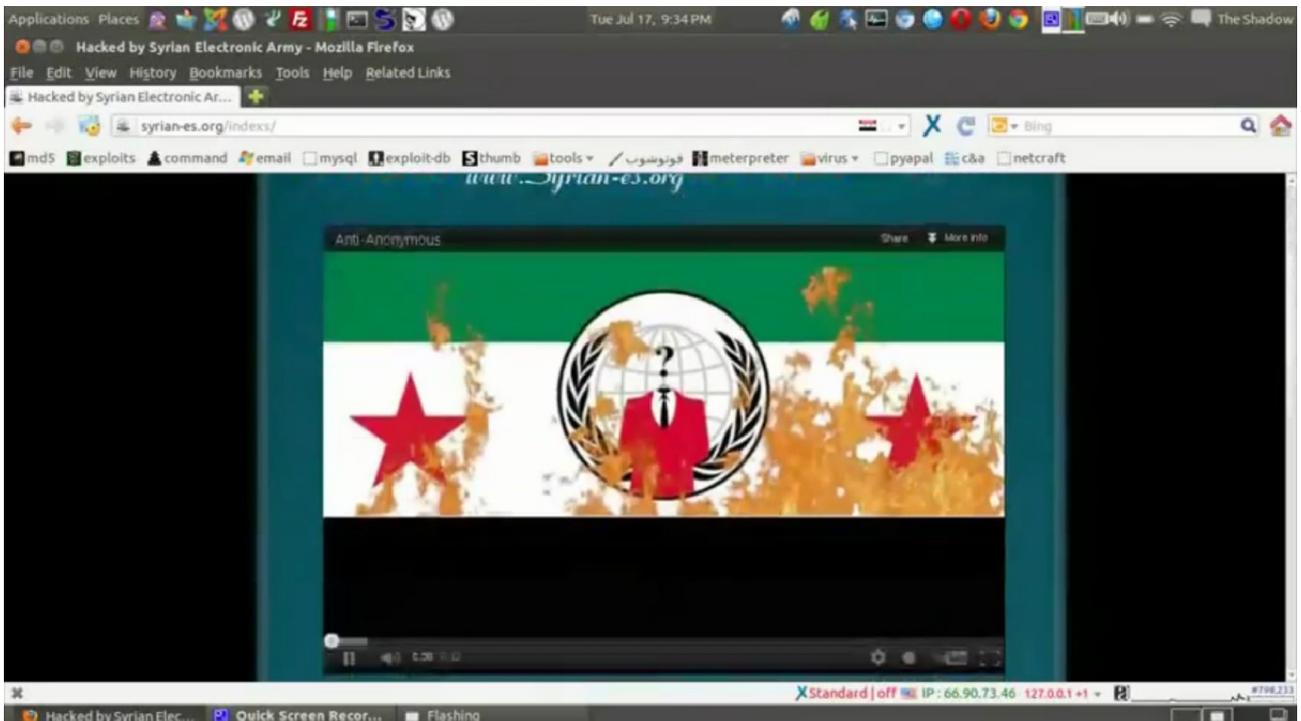
Frankly, both sides are a bit exhausted by the cyber war and I don't think you could say that there's any sort of battle plan other than to simply persevere and continue the fight. As long as they continue to support Assad, I think it's safe to say the SEA would do well to expect us to carry on.”⁸⁶

One screenshot from a message of Anonymous may illustrate the campaign mentioned in the interview:

86 http://www.vice.com/en_uk/read/the-syrian-electronic-army-hacked-the-bbc (accessed 05/05/2013).



SEA retaliated by defacing *anonymousnetherlands.nl*⁸⁷ and trying to disseminate counter-propaganda using an Anonymous framing.⁸⁸



Implicit threats of attacks against the SEA are voiced by other groups. The blog *ZionOps* hints at possibilities to hack the SEA site because it uses an older version of the content management system

87 <http://www.youtube.com/watch?v=q-7-XLJM4Ss> (accessed 05/05/2013).

88 <http://www.youtube.com/watch?v=2ODtjyYzEhA> (accessed 05/05/2013).

Joomla, “full of holes and an easy hack”. *ZionOps* mentioned other Syrian sites that may be vulnerable, too.⁸⁹

Against Assad's foes

On August 15th, 2012, two unknown groups – *Cutting Sword of Justice* and *Arab Youth Group* – claimed responsibility for a cyber attack on the Saudi Aramco, Saudi Arabia's oil company, aiming at the erasure of data on the computers of the company to stop the flow of oil and gas using malware called Shamoon^{90,91} The Qatari company RasGas, the top natural gas firm of the country, has been attacked less than two weeks later.⁹² The post reads:

“We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action.

One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people.”⁹³

We may read this attack as part of the activities to target the supporters of at least part of Syria's opposition, i. e., Saudi Arabia and Qatar. Using words like “Muslims oil resources” indicates other sources than the SEA. The *Arab Youth Group* called its attack “The companions of the prophet” using religious and Arab nationalist frames.⁹⁴

Later on allegations against Iran appeared but remained speculative.⁹⁵ The first information on the attack were apparently published by two Saudi sources. The first one at 6:17 pm described several effects of the attack⁹⁶, the second one referring to the first source mentioned at first “the state of Iran” (*daulat Iran*) as the source of the attack. But then the blogger, Sa'ud al-Hawawi, adds that

89 <http://zionops.wordpress.com/2012/02/08/syrian-electronic-army-is-open-to-hacking/> (accessed 04/20/2013).

90 “The attack is called “Shamoon,” due to a string of a folder name within the malware executable (“C:\Shamoon\ArabianGulf\wiper\release\wiper.pdb”).” (<http://www.seculert.com/blog/2012/08/shamoon-two-stage-targeted-attack.html>) (accessed 04/20/2013) Kaspersky Labs analysed it as the work of script kiddies inspired by former attacks in the Middle East (http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work (accessed 04/20/2013)).

91 <http://secureconnexion.wordpress.com/tag/cutting-sword-of-justice/> (accessed 04/20/2013)

92 http://news.cnet.com/8301-1009_3-57503641-83/virus-knocks-out-computers-at-qatari-gas-firm-rasgas/?part=rss&tag=feed&subj=News-Security&Privacy (accessed 04/20/2013)

93 <http://pastebin.com/HqAgaQRj> (accessed 04/20/2013)

94 The group claimed another attack at the Saudi Arabian stock exchange; <http://worldanalysis.net/modules/news/article.php?storyid=2168> (accessed 04/20/2013).

95 <http://analysisintelligence.com/cyber-defense/narrative-of-a-cyber-attack-saudi-aramco-and-shamoon/> (accessed 04/20/2013)

96 <http://sabq.org/Ynmfde> (accessed 04/20/2013)

“Iran has no connection to the attack.”⁹⁷

Trojans, Malware etc.

On February 17, 2013, *CNN* reports⁹⁸ regime supporters used stolen online identities of online activists, impersonate them, gain the trust of other activists and convince others to download a file. This file will install a trojan adapted for this campaign. The program uploads the information (passwords, contacts etc.) to a server of the state owned Syrian Telecommunication Establishment. The virus was passed off in a chat room used a fake Facebook logo. The virus was described by *netzpolitik.org* a modified version of the remote administration tool *darkcomet-rat*.⁹⁹ Another more complex virus was used, too.

There are other ways to spread a virus are used. On January 29, 2013, the activists supporting the uprising on *Telecomix: Syria* issued a warning in Arabic and English:

“Security warning: every page of the website www.syrian-martyrs.com asks the user to download a file named "ActiveX.exe". This file probably contains a virus, do not download it. The suspicious HTML code is added at the end of every page of the website as an iFrame containing the executable file. The website is normally legit, so it may have been hacked into. An antivirus detects viruses "Win32/Agent.BAD" and "PHP/C99Shell.H" in the ActiveX.exe file.”¹⁰⁰

The main activities of the SEA and other pro-regime electronic activists aim at spreading counter-propaganda to what is perceived as false news disseminated by non-Syrian media.

Leaks

E.g., online platforms providing newsbits that apparently didn't make it into mainstream media and trying to profit from the *Leaks*-Label popularized by *WikiLeaks* are used by pro-Assad activists for counter-propaganda. E.g., *LiveLeak* a platform publishing videos like “Dog bails from a car after accident!” from Uruguay, “This toy gun commercial would never be shown on T.V. Today” from the United States or “Pedestrian running the road hit by minibus” from Turkey are used by pro-regime activists to spread their views. They are calling themselves *trustedsource11*¹⁰¹ or *nutsflipped*.¹⁰²

97 <http://www.tech-wd.com/wd/2012/08/15/aramco-hacked/> (accessed 04/20/2013)

98 <http://edition.cnn.com/2012/02/17/tech/web/computer-virus-syria/> (accessed 03/28/2013)

99 <http://netzpolitik.soup.io/tag/Trojaner> (accessed 03/28/2013)

100 <http://syria.telecomix.org/545b157fca80ad968f4270b4c9f2a5ce> (accessed 03/28/2013)

101 The comments for this source revealing that the level of discussion is as sophisticated as in any other online forum.

102 For the YouTube channel *nuts flipped* see below. Anti-regime postings try to rebut a posting by *nutsflipped* in

Nutsflipped announces the reopening of his account on *LiveLeaks* using a video clip of Homer Simpson on January 25, 2013¹⁰³ demonstrating his intimate knowledge of global western mass culture and the audience he is aiming at. *Nutsflipped* tells about himself:

“I love Syria. I expose the lies of the mainstream media and terrorist organizations that target Syria. I am not affiliated with any organization or intelligence agency nor do I get any money for the work I do. This is a patriotic duty that I am doing.”

The discursive threads he is connecting to are: loving Syria – correcting media lies – not paid/working for intelligence agency – patriotic duty. All these elements can be found in other contributions discussed here.

QatarLeaks et al.

The SEA is not only present at online platforms like *LiveLeaks*. It is adopting the Leaks format for its own purposes. So it established a website called QatarLeaks as part of project aiming at publishing confidential documents from Qatar, Saudi-Arabia, Turkey and other Arab countries proving a conspiracy against Syria.¹⁰⁴ Entering the advertised *SEALeaks* site¹⁰⁵ the success is less impressive. The documents offered are from the diwan of the amir, the bureau of his wife, the foreign ministry, the League of Arab states.

Most of the documents are not as informative as advertised: a dossier for a visit of the then Italian prime minister, Mario Monti, in Qatar, recommendations for Qatari nationals treated at a hospital in Bangkok, visits of the foreign minister planned, a request for a meeting in New York, talks about the release of a Danish and Bahraini national, a visit of the minister of foreign affairs to East Asia, a meeting with the Chinese prime minister, meetings in New York on the occasion of the UN general assembly, a meeting of representatives of the Syrian opposition with representatives of several states in New York on the occasion of the UN general assembly. Not really breaking news since a press conference was to be held, presents for a visit in Paris at the UNESCO, a notice to media people about a meeting with the secretary general of the Arab League and the Turkish prime minister Erdogan just informing about date and place, the date of a Qatari-Arab League meeting, a short notice about a press release, a request for a meeting with the secretary general by the former president of the European Commission, Romano Prodi, a request by the Arab Organization for

http://www.liveleak.com/view?i=03c_1350246365 (accessed 03/28/2013).

103http://www.liveleak.com/view?i=c7d_1359151699 (accessed 03/28/2013).

104<http://www.islamicinvitationturkey.com/2013/01/07/syrian-electronic-army-to-publish-a-series-of-international-leaks/> (accessed 03/23/2013) and http://www.liveleak.com/view?i=2c2_1359237557 (accessed 03/23/2013)

105<http://leaks/syrian-es.org/> (accessed 03/23/2013)

Human rights on behalf of Syrian refugees in Algeria, a meeting of ministers of foreign affairs, another meeting. Personal communication to the secretary general, daily routine, files containing daily administrative routine: discussing coordination affairs, details about options referring to cars etc.

Much more interesting may be for the Syrian hackers files on the case of Libya, talks with the Iranian ambassador etc.

Another example: there are four fax messages: a) the emir of Qatar calling the Egyptian president Morsi talking about a visit of the emir of Qatar in Egypt and exchanging polite remarks b) administrative affairs of the Qatari embassy in Abu Dhabi c) administrative affairs of the consulate general of Qatar in Mumbai, and d) administrative affairs of the Qatari embassy in Jordan¹⁰⁶, the last three faxes purely daily business.

A new success, announced as a “quantum leap”, for the SEA is the publication in Arabic of an investigative book on Qatar written by two French authors.¹⁰⁷ Other new leaks generated documents about an Ukrainian journalist kidnapped in Syria and the negotiations between Qatar and the Ukraine.¹⁰⁸ Even the request from the office of Sheikha Moza to block the Leaks site of the SEA (now *leaks.sea.sy*) is documented.¹⁰⁹

YouTube

There are several videos on YouTube by the SEA using, e.g., the nickname *syrianes 0 to 2*. To mention just a few: “Reply from the Syrian Electronic Army to Anonymous”¹¹⁰, boasting the hack mentioned above, “Tutorial: How to use the Shell of the Syrian Electronic Army”¹¹¹ or a recruitment video.¹¹² Some screenshots:

106 Turned upside down.

107 <http://sea.sy/article/id/1965/en> (accessed 11/23/2013).

108 <http://sea.sy/article/id/1916/en> (accessed 11/23/2013).

109 <http://sea.sy/article/id/1972/ar>; part of the post does not work (accessed 11/23/2013).

110 <http://www.youtube.com/watch?v=D0T-uBJS-EI> (accessed 03/28/2013)

111 <http://www.youtube.com/watch?v=foD56TQbMEo> (accessed 03/28/2013); the shell will be discussed below.

112 http://www.youtube.com/watch?v=n_cyqJHa3hQ (accessed 03/28/2013)



Join the Syrian Electronic Army



The Shell working

Several channels at video platforms like *YouTube* are part of the efforts we are discussing here.

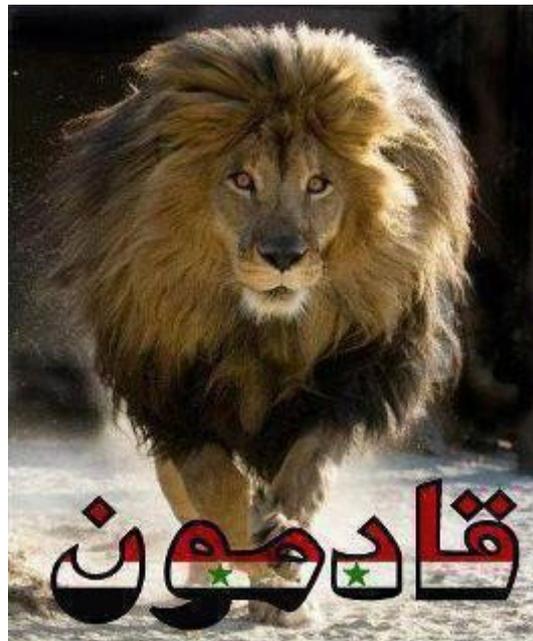
Nutsflipped, active on *LiveLeaks*, too, has a *YouTube* channel called *nuts flipped*, decrying

copyright by YouTube.¹¹³ The channel is active since March 27, 2012¹¹⁴, and got 144.321 hits (March 28, 2013) the majority of hits referring to three videos only, others get 3-400 up to 1000 hits, a limited audience.

Other pro-Assad activists use telling names like *Syria TruthNetwork*, *thesyrianfighter3*, *Syrians Worldwide* or *SuriComrade*.

Facebook

The current page of the SEA at Facebook using an interesting way of writing its name¹¹⁵ is offering counter-information, videos, postings ridiculing the enemies of the regime (cartoons etc.), singling out opposition pages, trying to create a positive image and displaying power. One of the picture is subtitled: "They are coming." and showing a male lion advancing, playing with the name of the family al-Assad, "the lion".



There is a small group of main contributors, one of them demonstrating his Russian affiliations, sympathy with pro-Assad Kurdish groups etc.

SEALeaks celebrated recently (2013-02-14) page no. 200 on Facebook; 199 Facebook pages of SEA have been closed by Facebook.¹¹⁶ Now it is number 256 (see above).

113<http://www.youtube.com/channel/UCf8tmm0hSmI3v3A2zgGIbtg> (accessed 03/228/2013)

114There are three other channels called *nuts flipped* with membership dates of March and April 2012.

115<http://www.facebook.com/groups/134916399952567/?fref=ts>

116<http://syrian-es.org/article.php?id=1906&lang=en> (accessed 03/23/2013)



Another media outlet is the Arab-English portal *Breaking News/Shabakat 'ajil al-ikhbariyya*.¹¹⁷ Part of the Syrian efforts to counter the rebellion are counter propaganda sites, e.g., on Facebook. like *al-Shabiha al-iliktruniyya* referring to militant loyalists¹¹⁸ often accused for their brutality with XXX “Likes”¹¹⁹, the fan-site of the ruling Baath party with XXX “Likes”¹²⁰. Other sites are *Mahbuba al-Assad*, a group for all people “loving al-Assad and his followers” or *Jabha al-mu'abbada*, “the eternal front”¹²¹, playing with the name of the jihadi organization *Jabhat al-nusra* or several “armies” mentioned below.

Th3 Pr0

The 18 year old Syrian hacker¹²² *Th3 Pr0*, mentioned above as “The Leader of Special Operations” of the SEA, has many online sites. His blog on *WordPress* is closed at the time of writing, one Twitter account is closed down, but he is running another one using the hashtag *@ThePro_Sy* often linking to his blog, another one is *Th3Pr0_SEA*, still active at least at April 30, 2013. His YouTube channel *ThePro112233*¹²³, announcing successful hacks, is inactive since January 2012. He is active at Google+ as *Syrian Pro* and at Foursquare as *Th3Pr0 S.*; at Google+ he is linked to a member of the *Baath Electronic Army*, a modestly active outfit¹²⁴:

¹¹⁷<http://www.breakingnews.sy/ar.html> (accessed 03/09/2013).

¹¹⁸ Another Facebook site is *Shabihat al-Asad*, <https://www.facebook.com/Shabii7a?fref=ts> (05/05/2013).

¹¹⁹16.662 “Likes”, August 2012 (Lohlker/Telič 2013, p.183).

¹²⁰13.385 “Likes”, August 2012 (Lohlker/Telič 2013, p.183).

¹²¹No more available on Facebook.

¹²²<http://about.me/Th3Pr0> (accessed 05/05/2013).

¹²³<http://www.youtube.com/user/thepro112233> (accessed 05/05/2013).

¹²⁴With nice effects on <http://gardermo.net/> (accessed 05/05/2013), see also <http://www.zone-h.org/archive/notifier=>



At Foursquare it is 13 friends, one of his Twitter accounts has 46 followers, his YouTube channel at maximum around 1400 clicks. His main activity is by now on Facebook

Other activists of the SEA are *SEA The-Shadow*, “Leader in Syrian Electronic Army”¹²⁵, and *Vict0r*, “The Leader of Programming Depart in Syrian Electronic Army”.¹²⁶

Members of the SEA killed and captured

The SEA has a sub-site dedicated to two members killed in Idlib and the other one in a place not mentioned. It is not quite clear why they were killed, as members of the SEA or supporters of the Syrian regime.¹²⁷ Since there are other indicators demonstrating the intimate knowledge of the persons acting (see below). So a direct attack appears to be possible.

A YouTube video was posted showing a man called SyRiAn_34G13¹²⁸, introduced in the text as co-founder of the SEA with Pr0¹²⁹, the interviewee from the SEA mentioned above. He is described as the programmer of the *Syria Shell*.¹³⁰

¹²⁵https://twitter.com/Th3Shadow_SEA (accessed 05/05/2013).

¹²⁶https://twitter.com/Vict0r_SEA (accessed 05/05/2013).

¹²⁷<http://syrian-es.org/section.php?id=9&lang=ar> (accessed 03/28/2013).

¹²⁸A person using the same acronym is registered at *Romanian Security Team*. (https://rstforums.com/forum/members/syrian_34g13/ (accessed 05/04/2013)).

¹²⁹Who is threatened, too.

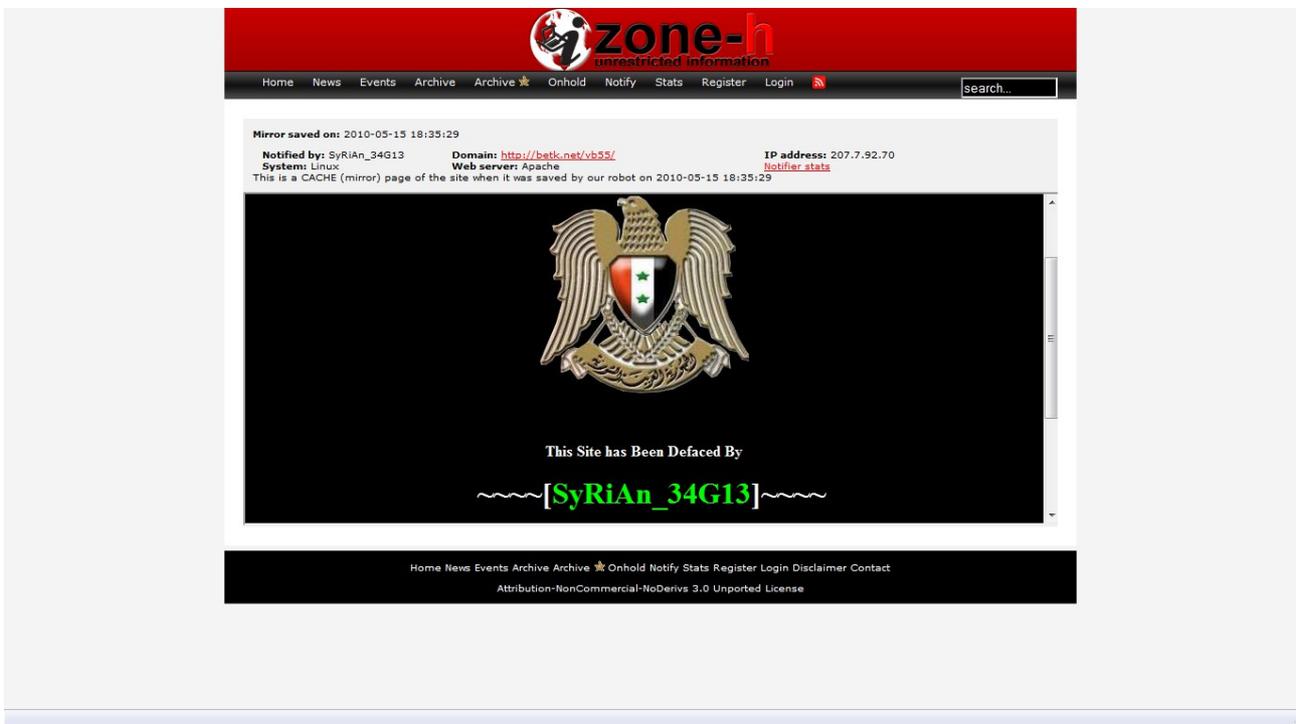
¹³⁰<https://github.com/nikicat/web-malware-collection/blob/master/Backdoors/PHP/SyRiAn.Sh3ll.v7.txt> (accessed 05/04/2013) and <http://bot24.blogspot.co.at/2012/09/syria-shell-v7-script.html> (accessed 05/04/2013). Notice the shape of a gun at the beginning of the code.



Until April 28, 2013, these hackers defaced 92 websites.¹³⁴

SyRiAn_34G13 worked together with a guy calling himself G705T H4CK3r notifying 21 defacements.¹³⁵

The mirrors on *zone-h.org* notified by SyRiAn_34G13 show in 2010 the aesthetics used by the SEA:



In 2013 the defacements have changed from the time of the original SyRiAn_34G13, greeting other hackers,

¹³⁴<http://evuln.com/labs/hackedby/210/> (accessed 05/04/2013).

¹³⁵<http://www.zone-h.org/archive/notifier=G705T%20H4CK3r> (accessed 05/04/2013).

one of them a collaborator of the *Syrian Shell*.¹³⁶

May 15, 2012, the SEA claimed the release¹³⁷ of an official SEA shell, based evidently on the *Syrian Shell*.¹³⁸

Threats against anti-regime activists

Virtual activities are connected by real life actions. There are reports of threats against Syrian opposition activists trying to force them to go offline.¹³⁹ Non Syrian supporters of the Syrian uprising like *Telecomix* have been threatened, too.¹⁴⁰ Newspaper articles tell, activists are being tortured to obtain their passwords.¹⁴¹

A significant story is reported by a founding member of the *Pirates of Aleppo* an anti-regime hacktivist group:

“The young software developer started on this path in the early days of the Syrian uprising by uploading to YouTube under the moniker “Harvester” videos of demonstrations with English subtitles, in the hope that those on the outside would come to understand the events taking place in his country. In the summer of 2011, as the demonstrations became a daily occurrence and the regime sought to stamp out dissent with a heavy hand, Ahmad, like many young people who had studied computer science in Syria, was approached by a regime-sponsored organisation calling itself the Syrian Electronic Army.

'A friend of mine was already working with them,' he explained, 'and he took me along to their operations centre, hoping to sign me up. It was like a normal computer shop in the front, but at the back there were stairs leading down to a basement where I discovered another world: rows of routers and high-spec machines, including American-made components I'd never seen in Syria before, all serving one huge domain. They were using this technology to track activists' IP addresses, so the police and army could locate their homes.'"¹⁴²

When one of the activists was arrested, he was tortured and revealed the names of the other activists. He was released, all his fingers cut off during torture. The group dissolved and the members fled to Turkey, Russia, and Saudi-Arabia (Schaap 2013: 62).

136<http://www.zone-h.org/mirror/id/19273878> (accessed 05/04/2013).

137<http://blog.thepro.sy/News/Content/Show/Node-ID/764> (accessed 07/12/2012), now offline.

138For the tutorial v. above the section on YouTube.

139Personal communication October 2012.

140<http://www.dradio.de/dlf/sendungen/dlfmagazin/1698650/> (accessed 03/22/2013).

141<http://www.welt.de/politik/ausland/article13403475/Syriens-Cyber-Miliz-steht-auf-verlorenem-Posten.html> (accessed 03/22/2013)

142<http://www.irishtimes.com/news/online-pirate-army-fights-for-downfall-of-assad-1.3891> (accessed 05/01/2013)

The Syrian opposition acquired electronic armies, too. E. g., the *Jaysh Homs al-iliktruni*, the “Electronic Army of Homs”, has a Facebook group promoting videos, or the “Electronic Army of Bab al-Tabbana”, a quarter of Tripoli in North Lebanon, *Jaysh Bab al-Tabbana a-iliktruni*, sporting as a mission statement the fight against pro-Assad sites.¹⁴³ Other armies, closer to the regime, are also present at Facebook: *Jaysh al-watan* or *Jaysh al-sahil al-watani* may be mentioned.

Bibliography

- Gonzalez-Quijano, Yves (2012), *Arabités numériques. Le printemps du Web arabe*, Paris: Sindbad
- Information Warfare Monitor (2011), *Syrian Electronic Army: Disruptive Attacks and Hyped Targets* (<http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/>) (accessed 04/03/2013)
- Kirchner, Henner (2003), “Cyberintifada? Internet-Nutzung in der Auseinandersetzung zwischen Israeli und Palästinensern”, in Martin Tamcke (ed.), *Orient am Scheideweg*, Hamburg: Verlag Dr. Kovač, pp. 263-275
- Lohlker, Rüdiger/Telič, Anna (2013), Die Rolle von »Social Media« in der syrischen Revolution, in Fritz Edlinger/Tyma Kraitt (eds.), *Syrien: Hintergründe, Analysen, Berichte*, Vienna: Promedia, pp.175-187
- Noman, Helmi (2011), *The Emergence of Open and Organized Pro-Government Cyberattacks in the Middle East: The Case of the Syrian Electronic Army* (<http://www.infowar-monitor.net/2011/05/7349/>) (accessed 04/03/2013)
- Paget, François (2012), *Hacktivism: Cyberspace has become the new medium for political voices* (<http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf>) (accessed 04/05/2013)
- Passeri, Paolo (2011a), *Tweets like Weapons* (<http://hackmageddon.com/2011/07/>) (accessed 03/22/2013)
- Passeri, Paolo (2011b), *Consumerization of Warfare 2.0* (<http://hackmageddon.com/2011/06/21/consumerization-of-warfare-2-0/>) (accessed 03/22/2013)
- Schaap, Fritz (2013), “Zimmer mit Krieg”, in *Datum 5*, pp.58-65
- Villeneuve, Nart (2010). *Koobface: Inside a Crimeware Network*, November 12, 2010 (<http://www.infowar-monitor.net/reports/iwm-koobface.pdf>) (accessed 03/23/2013)
- York, Jillian C. (2011), *Twitter Trolling as Propaganda Tactic: Bahrain and Syria* (<http://jilliancnyork.com/tag/syrian-electronic-army/>) (accessed 04/03/2013)
- Zapparoli Manzoni, Andrea/Passeri, Paolo (2011), *Consumerization of Warfare* (<http://hackmageddon.com/2011/06/16/consumerization-of-warfare/>) (accessed 03/22/2013)

¹⁴³For these hacking attacks of both sides see, e.g., Jillian C. York on Al-Jazeera opinion page (<http://www.aljazeera.com/indepth/opinion/2011/08/201181191530456997.html>) (accessed 04/03/2013).