Received 15 December 2015
Accepted 10 March 2016

The Syrian Electronic Army – a hacktivist group

Matthew Warren
Deakin University Centre for Cyber Security Research, Deakin University, Melbourne, Australia, and
Shona Leitch
College of Business, RMIT University, Melbourne, Australia

Abstract

Purpose – The aim of the paper is to assess the hacktivist group called the Syrian Electronic Army and determine what their motivations in terms of ethical and poetical motivations.

Design/methodology/approach – This paper looks at chronological examples of Syrian Electronic Army activities and assess them using a developed hacktivist criteria to try and gain a greater understanding of the motivations of the Syrian Electronic Army. The paper uses a netnography research approach.

Findings – This paper determines that the Syrian Electronic Army is motivated to protect the Syrian Government. This protection is highlighted by the new media and social media organisations that the Syrian Electronic Army attacks online.

Research limitations/implications – This paper focuses only on one group the Syrian Electronic Army.

Practical implications – A greater understanding of the Syrian Electronic Army.

Social implications – A greater understanding of the development of hacktivism.

Originality/value – A unique study into the motivation of the Syrian Electronic Army.

Keywords Ethics, Netnography, Hacking, Socio-politics

Paper type Research paper

Introduction

We have seen a rise in computer misuse at a global level; In many cases "Hackers" have been found responsible for these attacks[1]. Hackers are often characterised as adolescent males in dark bedrooms that can cause damage to global information technology systems through using their computers and computer skills. A more romantic perception portrays hackers as being determined cyber knights, who use personal codes of conduct to live by and are reminiscent of the great Arthurian knights (Warren and Hutchinson, 2003). Moreover, "hacker" is what computer intruders choose to call themselves, not as a criminal pejorative, but as a noble title given to those "soaked through with heroic anti-bureaucratic sentiment" (Sterling, 1993). Hacking then, can describe the determination to make access to computers and information as free as possible. Hacking can involve the heartfelt conviction that beauty can be found in computers, that the fine aesthetic in a perfect program can liberate the mind and the spirit (Levy, 1984).

Contrasting this romantic perception is the way Sterling (1993) portrays "Hacking" in his book titled *The Hacker Crackdown*. In Sterling's (1993) book, "Hacking" is described

Journal of Information, Communication and Ethics in Society
Vol. 14 No. 2, 2016
pp. 200-212

1477-996X
DOI 10.1108/JICES-12-2015-0042

as the act of intruding into computer systems by stealth and without permission. However, Sterling's definition of "Hacking" is broader than the one used routinely by most enforcement officials with any professional interest in computer fraud and computer abuse. The enforcement officials' focus on "Hacking" relates to crimes committed with, by, through or against a computer (Warren and Hutchinson, 2003).

As has been demonstrated, the perception of "Hacking" is dependent on personal and ethical perspectives. This paper looks at the development of hacktivism and the evolution of one key, emerging group, the Syrian Electronic Army (SEA). The paper will discuss the SEA's ethical actions and how this has impacted their existence and operations. The key research question to be examined in this paper is whether the actions of the SEA are ethical.

Hackers a historical background

The original hackers and their activities from the 1960s and 1970s are discussed by Levy (1984) in the book *Hackers: Heroes of the Computer Revolution*. The first "hacktivist" attack occurred in 1989, from a computer in Melbourne, Australia. The hacktivists involved were opposed to nuclear weapons, sending a WANK (Worms Against Nuclear Killers) worm as a protest to infect targeted computers with a login logo "Your System Has Been Officially Wanked". Targeted computers include the US Department of Energy and NASA, but source code specifically did not target New Zealand computers, as a support to their anti-nuclear position (Hanna, 2013).

The prominent hacktivist groups of the 1990s were the Cult of the Dead Cow, L0pht and the Hong Kong Blondes. These groups are strictly ideological, condemning politically motivated activities such as website defacement or DDoS (Distributed Denial of Service) attacks undertaken by other hacktivists (D'Amico, 1999; Hanna, 2013). In 1989, Legions of the Underground attempted to begin cyber-attacks against China and Iraq, hoping to disrupt the information infrastructure of these countries; however, after the prominent hacktivist communities of the time oppose their attack, Legions of the Underground cancelled their plans (Hanna, 2013).

The hacktivist members of Cult of the Dead Cow produce the "Hacktivismo Declaration", in 2001, which championed human rights and freedom of information through technology as a democratic right (Hanna, 2013). However, hacktivists spawned from 4chan's "no rules" board did not conform to this declaration and the group Anonymous was born (Hanna, 2013).

Since 2003, Anonymous has grown from being a group of pranksters and trolls on 4chan to becoming politically and socially motivated hackers (Hanna, 2013). Anonymous uses cyber-attacks aimed at corporations, government and religious entities to convey their discontent at internet freedom (Li, 2013). Regarding the US Government, Anonymous opposes the "overaggressive enforcement of intellectual property, cybersecurity, and computer crime laws" (Benkler, 2012). One Anonymous supporter believes the strength of Anonymous that it is not a traditional group, but rather an ideology. However, Gabriella Coleman reinforces the notion of viewing Anonymous as a group. Coleman (Bryan-Low and Gorman, 2011) views Anonymous as a group with decentralised nodes of power. In 2010, Anonymous played a crucial role in the Arab Spring regarding using DDoS attacks, "an action that prevents access to a Web site for several hours"). In this instance, Anonymous participants engage in online sit-ins where they disrupt a website temporarily (Benkler, 2012) by targeting a server

and overloading it with information requests (Adams, 2013). They also provide digital training and encryption software for protestors to evade government officials and widely disseminate videos of protestors, in an attempt to support their goal of defending internet freedom (Adams, 2013).

In February 2011, Anonymous members took part in attacking the internet security company, HBGary Federal. Anonymous obtained and released thousands of internal emails in retaliation for Aaron Barr, CEO of HBGary Federal, who had exposed the identities of Anonymous' leaders. This action by some Anonymous members causes internal friction within Anonymous and results in a splinter group, Lulzsec, being formed. Lulzsec's focus was not politically or socially motivated, providing instead a platform for members to showcase their hacking ability (Bryan-Low and Gorman, 2011; Adams, 2013).

The recent development of hacktivism

The origins of hacktivism are a movement that engages a largely apolitical generation into taking political action through fun. The political action involves engaging in technologically advanced libertarian attacks (Hanna, 2013). There is not one ideology that hacktivists follow. It appears that a large number of hacktivists are libertarians who are anti-authority and pro "human rights, privacy and pacifism"; however, there are also those that are anarchists and anti-capitalist (Hanna, 2013). Common themes amongst hacktivists seem to be the desire for internet freedom; the desire for increased government transparency; they do not seek financial gain, they may seek revenge; and they engage in civil disobedience (although some do engage in cyber-crime); and they wish to disclose their activities and hacking methodology publically (Held, 2012).

The historical review of hacktivism illustrates how hacktivist ethical parameters have evolved since the 1990s. In the 1990s, hacktivism championed human rights and freedom of information with hacktivist activities mirroring these values. More recently, hacktivist activities demonstrate either *traditionalist* or *expansionist* values. Tavani (2005) summarises *traditionalists* (also known as *instrumentalists*) hacktivism values as utilising a "system that is composed of normative principles, rules and theories". Because of history showing most media eventually conform to government control until now it has been assumed that the ethical principles of hacktivists on the internet would align within an "existing ethical framework" (Held, 2012). The normative principles particularly suit government objectives that aspire for the internet to be utilised as a vehicle of harm against governments as highlighted by the practice of hacktivism (Sterner, 2011).

In contrast with traditionalists, expansionists or internet freedom fighters (confederates) take the opposite position. Expansionist goals are to decentralise the internet, seek freedom of information and increased government transparency. Although expansionists may attack individually, their hacktivist goals are part of a long internet war (Hwang, 2010) and the pursuit of internet freedom. An expansionist example is the software patent access attacks in the 1980s, Napster and Bit Torrent's copyright law attacks and WikiLeaks' copyright content challenges. These all constitute individual attacks that have the objective of progressing internet freedom (Hwang, 2010; Held, 2012). Sterner (2011) reinforces Hwang's expansionist claims, asserting internet freedom fighters are hoping to create a new society with greater liberty. Anonymous actors believe the actions they take should result in greater societal

freedom, per Sterner's (2011) position. Additionally, Anonymous participants feel the cyber-attacks they make are proportional to the motivations and purpose of the attack. For example, Anonymous members may take part in a DDoS cyber-attack. Here, an Anonymous member participates illegally in occupying and disrupting a website. However, they view the website defacement and non-cyber action as pranks. The most serious of their attack types, document disclosure, are reserved for organisations that Anonymous views as abusing their power. Through the use of document disclosure, Anonymous try to highlight that powerful organisations are societal gatekeepers that also need surveillance for transparency and accountability purposes (Benkler, 2012). As Benkler describes, the actions taken by Anonymous can be understood as being ethically motivated.

Aside from demonstrating ethical values through hacktivism, hacktivism can be understood in the context of the US constitutional, first amendment. Li's (2013) study deals with this, using a legal empirical report. Li asserts that hacktivism "involves the use of technology hacking mechanisms, often in the form of cyber-attacks, to effect particular political and social change" (Li, 2013). Despite cyber-attacks being outlawed under the US Computer Fraud and Abuse Act of 1986 (Li, 2013), Anonymous debate that their hacktivism is illegal, Anonymous position their cyber-attacks as the equivalent of political "sit-ins". This position is directly opposed by most government agencies, for example, Keith Alexander the National Security Agency Director and General in charge of the US Cyber Command; US Department of Homeland Security and the media, who publicly describe Anonymous as being terrorists (Benkler, 2012).

Li (2013) argues that some modified form of hacktivism may evolve that allows for free speech utilising a "cyber sidewalk" that operates adjacent to the target's online property. A development of this sort may alleviate the current legal constraints that currently impinge on first amendments rights. However, "cyber sidewalks" may remove the current anonymity hacktivism provides, along with the "free exchange of ideas" (Hanna, 2013). Hanna (2013) argues that the anonymity provided by hacking identities allows for hacktivists to take a political position free of personality politics. This anonymity allows for the essence of the message to get across in the public sphere. Where anonymity does not prevail, as has occurred with Julian Assange and Edward Snowden, there seems to have been a dilution of their political messages. Instead, the focus has been on their personalities and lives, which have been dissected. Nonetheless, it would be difficult to quantify whether losing their anonymity has negatively impacted their political cause. Despite Assange and Snowden's public personas, they still advocate for the freedom of the internet and government transparency.

Tactics used by hacktivists

Hacktivists tend to break into computer networks to retrieve data and then announce their work to try and obtain support for their political point of view (Turner, 2014; Held, 2012; Peters, 2013). Hacktivist activity seems to be driven by an anti-government agenda. Hacktivists hope to expose truths to the public about what is happening in mainstay institutions (Held, 2012) and, for the most part, hacktivists "operate in flat, open-ended associations" (Conway, 2007), such as Anonymous.

Benkler (2012) postures that Anonymous' activities could be legitimised as a civil engagement platform that attempts to ensure the purpose of the internet continues. That

is, creativity, expression and innovation are continued. Benkler's developed a list that describes the common attack types Anonymous use; these are shown in Table I.

Syrian electronic army

The SEA are a group of non-partisan Syrian computer hackers. The SEA was launched in 2011. The SEA's main political agenda is to counter Arabian and Western media portrayals of the Syrian uprising (2011), which the SEA feel sabotage the world view of the role of the Syrian Arab Army. The SEA also use hacking to support the Syrian President Bashar al-Assad and his government. Their strategy is (iGmena, 2014):

- target and attack western groups (including corporations and government websites) politically opposed to Syrian President Bashar al-Assad's position being reinstated; and
- hack social networking sites of famous people who oppose Bashar al-Assad.

Despite the non-partisan claims, the SEA's generic domain name was initially controlled by the Syrian domain name registrar. However, presumably with President Bashar al-Assad's support, the SEA current generic .sy domain name is hosted by the Syrian Computer Society (which was founded by the al-Assad family) (iGmena, 2014.). The SEA's links with Bashar al-Assad date back to the SEA formation. This gives a strong indication that the SEA may be run under the auspice of the Syrian Computer Society, which has been led by Bashar al-Assad since the 1990s (Hall *et al.*, 2013).

Syrian electronic army: hacktivism and cyberterrorism

The SEA has not attracted much academic attention and in isolation may continue to be seen as hacktivists with a propaganda agenda. However, with the Syrian Uprising becoming a Civil War (from 2011), the role the SEA play seems to have a greater importance in raising awareness of the Syrian Government. One questions whether SEA should be viewed as hacktivists or cyber terrorists. Additionally, are they a new brand of hacktivism and what are their ethical motivations?

The SEA timeline of hacktivist activity has been developed and assessed using the SEA's social media channels and traditional media sources (Table IV). However, this timeline only records the overt hacktivist agenda, not the covert intelligence agenda that the American intelligence community ascribes to this group (Taddeo, 2012). Covert activity is not usually a feature ascribed to hacktivism. Further complicating the notion of what hacktivism is the SEA operates as a hierarchical group, whereas traditional hacktivist groups seem to be flat (Al-Rawi, 2014).

Table I.
Anonymous attack types

Anonymous attack types	Purpose
DDoS	Sit-in/symbolic
Information disclosure	Transparency/accountability
Website defacements/electronic graffiti	Protest
Non-cyber action/pranks	Protest

Source: Benkler (2012)

Hacktivism is defined by Li (2013) as "it involves the use of technology hacking mechanisms, often in the form of cyber -ttacks, to effect particular political and social change". Denning's (2001) interpretation of cyber terrorism states that:

> […] operations that use hacking techniques against organisations Internet sites with the intent of disrupting normal operations but not causing serious damage. Examples are web sit-in and virtual blockades, automated email bombs, web hacks, computer break-ins, and computer viruses and worms.

The SEA does have a political agenda that they display during traditional hacktivist activity; this paper queries whether the SEA's role is only as hacktivists, because of their activities extending beyond how hacktivism has been characterised. Denning's interpretation of cyber terrorism is it is:

> […] 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).

By this definition, the Twitter announcement the SEA made which resulted in the stock exchange plummeting for a small period would define the SEA as cyber terrorists. Weimann's (2005) interpretation of cyber terrorism is a broader definition "the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)". There is no available evidence of the SEA engaging in these activities (from 2011 onwards) and although some intelligence experts believe they are cyber terrorists, a timeline of cyber-attacks from NATO's Review Magazine (2013) does not list the SEA's activities as having cyber significance.

Al-Rawi (2014) argues that the SEA is a cyber-terrorist organisation, rather than an hacktivist group acting under the direction of the Syrian Government with the dual purposes of being a public relations arm of the government and collecting intelligence on the Syrian opposition. It seems that the SEA is less interested in freedom of information than other hacktivist groups. For example, their Facebook pages and YouTube channels are moderated to remove anti-Assad content. Other claims that Al-Rawi (2014) makes which supports his cyber-terrorist claims are a tenuous link between the Syrian Government and SEA, which politically advantages the Syrian Government. It is unclear whether all the SEA recruits support the Syrian Government, or whether they join to receive the accolades of belonging to a hacker group. Nonetheless, Anonymous' operation #OpSyria exposed five SEA members who were located in Syria as well as Romania and Russia (Al-Rawi, 2014), pointing to the SEA not necessarily being located in Syria.

It cannot be said all of SEA's activities are hacktivist in nature, as not all of SEA's activities are overt. Some covert attacks have taken place as well (Al-Rawi, 2014):

- SEA used malware was used to collect 11,000 names and passwords of members of opposition groups, which was published in July 2012.
- Truecaller (on 17 July 2013) and Viber (23 July 2013) was hacked by SEA, and although what information was taken has not been confirmed, this could result in negative outcomes (e.g. copies of online conversations) for Syria's opposition members.

These covert SEA operations were focused on trying to steal information relating to opponents of the current Syrian Government. But as we can see in the next section of the paper, news outlets became key targets for the SEA cyber-attacks (Walker, 2013).

A key dimension of the SEA is the use of social media as a method of promoting their political agenda and details of their activities. The SEA Web and social media activities are shown in Table II.

Some of the major global social media companies, for example, Facebook and Instagram, have been successful in closing down SEA accounts, but other companies such as Twitter have closed accounts but this has not stopped the SEA from opening new Twitter accounts.

Research method

The complex nature of researching groups such as the SEA means that traditional research methods would not be applicable, so alternative research methods had to be selected. The complexity of the research is in part because of the fact that the actions of the SEA are in the cyber domain and not necessarily the physical domain. The complexity relates to the activities of SEA in a public and private online manner and via their use of social media.

The researchers determined that netnography would be a suitable research method for this piece of research because it is an online research technique for providing insight (Kozinets, 2002). Netnography adapts common participant observation ethnographic procedures to the unique contingencies of computer-meditated social interactions (Kozinets, 2010).

The research method used had the following stages:

- *Step 1*: Definition of Research Question, Social Sites or Topics to Investigate.
- *Step 2*: Community Identification and Selection.
- *Step 3*: Community Participation and Observation.
- *Step 4*: Data Analytics and Interpretation of Findings.
- *Step 5*: Write, Present and Report.

Table II.
Syrian electronic army web and social media activities

Platform	Address	Online November 2015
Website	http://sea.sy/	No
Facebook	www.facebook.com/sea.sy/facebook	No
Twitter	https://twitter.com/official_sea16	Yes
YouTube	www.youtube.com/user/SEAOfficialChannel	Yes
Google+	https://plus.google.com/101738095095683897710/videos	Yes
Pinterest	www.pinterest.com/officialsea/	Yes
Instagram	https://instagram.com/official_sea2/	No
VK (VKontakte)	http://vk.com/syrianelectronicarmy	Yes
Ello	https://ello.co/syrianelectronicarmy	Yes

Aligning these stages to the research in this paper was key to being able to collect and analyse the varied components appropriately. The specifics of each stage are detailed below.

(1) *Step 1. Definition of research question, social sites or topics to investigate*: This took the form of researching the activities of SEA online and commenced with the evaluation of media stories and identifying the social media sites that the SEA engage with and use to share information.

(2) *Step 2. Community identification and selection*: The social media channels that SEA used were identified (Table II) and the type of media outlets that would be monitored were defined.

(3) *Step 3. Community participation and observation*: This took the form of a longitudinal study and took the form of evaluating SEA by cross-referencing social media commentary with reports of their activities in the media.

The observation was of a passive nature and the researchers never posted or interacted via any of the SEA social media channels.

(4) *Step 4. Data analytics and interpretation of findings*: The analysis took the form of a number of steps. The complexity of the study warranted a number of different analytical approaches:

- An SEA attack criteria was developed to attempt to describe the online activities.
- A timeline of SEA attacks was formulated to show the types and nature of SEA attacks over an extended period. The aim was to describe complex events of a sustained period and linked to the attack criteria that had been developed.

(5) *Step 5. Write, present and report*: The research findings are presented in this paper.

The use of the netnography approach allowed for a comprehensive investigation and evaluation to be conducted and the results presented.

Timeline of SEA online attack

The following section is based on SEA-related Facebook pages (Facebook, 2015), and the analysis of SEA social media accounts (Syrian Electronic Army, 2015) as described in the research method section. The analysis took the form of looking at the history of SEA attacks and the type of attacks that occurred. The analysis of the SEA attack types is presented in Table III.

The netnography approach highlighted some interesting aspects specifically when cross-referencing the SEA attack claims in social media against media reports. There were numerous instances where the SEA made claims that could not be validated by media reports or other sources and therefore were not included in the research.

Additional problems occurred when SEA social media accounts were permanently closed, e.g. SEA Facebook account or when information channels were closed temporally, e.g. SEA Twitter accounts and SEA recreated new Twitter accounts.

The following (Table IV) is a list of SEA attacks linked to the organisational type, country and the attack type used.

Serial no.	Attack type	Description
1	Site redirect	The source site is redirected to different sites promoting SEA
2	Information theft	SEA steals online information and data
3	Defaced website	The website front pages are defaced with a pro-SEA logo and pro-Syrian government message
4	Account login details compromised	Captures user login details, e.g. social media accounts, and takes over user account, e.g. posting false information or messages
5	Mobile apps compromised	Organisational mobile apps are compromised at third-party hosting sites. Users then install infected apps on their mobile devices
6	Caused an individual website to stop working	Stopping access to view individual websites via directed attack, e.g. DDOS attacks, that slow down the operation and functionality of the attacked websites

Table III.
SEA attack types

As shown by Table IV, there has been a development in the sophistication and the attack ability of SEA. The early SEA attacks were focused on defacing websites, but the SEA have since developed the ability to steal specific social media login details, e.g. Twitter and post false information on social media; the ability to steal information; and as the ability to infect mobile applications on app stores. The SEA attack strategy has developed in sophistication when compared to the attacks carried out by groups such as Anonymous (Benkler, 2012).

The organisations that the SEA chose to attack is of interest. Many of the SEA attacks were focused on western news outlets, with the choice of attack related to those outlets that ran negative stories about President Bashar al-Assad and the Syrian Government. The attacks on social media outlets ensure that the news of their attacks is widely reported. Some of the organisations that have been selected for attack seem to be random targets of opportunity, e.g. the sporting organisations hacked in 2014.

Discussion

Although the SEA are labelled as hacktivists and meet many of the hacktivist criteria, their agenda does not support internet freedom for those who with differing political opinions or the desire for increased government transparency. So much of hacktivist history has been about championing social justice issues, especially human rights and technological freedom of information. However, the SEA has harnessed these technological tools to engage seemingly in propaganda and oppression (Hall *et al.*, 2013).

Leyden (2013) notes that the purpose of the SEA's attack on a "jobs website" that was operated by the US Marines Recruiting Command in early September 2013 was to leave a propaganda message. This attack was in retaliation for US President Barack Obama's announcement that he was seeking Congressional approval for a military strike on Syria, in response to reports that the Assad regime is using chemical weapons against the Syrian people. Many of the "victories" lauded on social media sites are not particularly sophisticated attacks, but rather a way of getting their message across and generating media attention for the SEA cause and the Syrian Government.

It is doubtful that Benkler (2012) would support SEAs activities in the same way as Anonymous activities, as their objectives do not seem to be about creativity and

Year	Organisation name	Organisation type	Country	Attack type
2011	University of California	Education	USA	3
2011	Harvard University	Education	USA	3
2012	LinkedIn	Social media	USA	1
2012	Twitter account of Reuters	Social media/News	USA/USA	4
2013	Gamerfood	Software company	USA	3
2013	Twitter account of Associated Press	Social media/News	USA/USA	4
2013	Twitter account of The Onion	Social media	USA	4,5
2013	Twitter account of ITV News	Social media/News	USA/UK	4
2013	Sky News	News	UK	5
2013	TrueCaller	Software company	Sweden	2
2013	Viber	Software company	Japan	2,3
2013	Outbrain	Information provider	USA	1
2013	New York Times	News	USA	1
2013	Twitter	Social media	USA	4
2013	New York Times	News	USA	6
2013	Huffington Post	News	USA	6
2013	Twitter	Social media	USA	6
2013	US Marine Corps	Military	USA	3
2013	Twitter/Global Post	Social media/News	USA/USA	4,3
2013	Google/Organizing for Action	IT company/News	USA/USA	4,1
2013	Vice	News	USA	1
2014	Facebook/Twitter/Skype	Social media/software company	USA/USA	4
2014	Twitter/Xbox	Social media/software company	USA/USA	4
2014	Microsoft	IT company	USA	3
2014	Twitter/CNN	Social media/News	USA/USA	4
2014	Ebay/Paypal	E-commerce/finical payments	USA/USA	4
2014	Facebook	Social media	USA	4
2014	Twitter/Forbes	Social media/News	USA/USA	4
2014	The Sun/Sunday Times	News/News	UK/UK	3
2014	Reuters	News	USA	3
2014	Chicago Tribune/CNBC/Forbes	News/News/News	USA/Canada/USA	1
2014	PC World	News	USA	1
2014	The Independent/The Telegraph	News/News	UK	1
2014	Toulouse FC	Sport	France	1
2014	National Hockey League	Sport	USA	1
2015	Le Monde	News	France	4,6
2015	Washington Post	News	USA	3

Table IV. Chronological breakdown of SEA attacks

innovation. It seems their actions may not be guided by a loose association of individuals, but rather coordinated by a centralised agency. Another aspect about the SEA is that their agenda is pro-Syrian Government and operates in organised manner; the extensive number of attacks as discussed in Table IV highlights this.

Returning to the research question of whether the actions of the SEA were ethical, it is clear that the SEA themselves do believe that they operated in an ethical manner, but that ethical stance and belief is linked to a very strong political motivation. This strong political motivation is very different from the political motivation of groups such as Anonymous, who align themselves more broadly and are linked to a wide number of different political causes. But other entities, e.g. Western Governments and media

outlets, believe that the SEA have not been ethical in their behaviour and their actions could instead be described as being criminal in nature.

It is clear that there is no simple way to determine whether the SEA have behaved ethically or otherwise, the complex situation had meant that some entities believe that the SEA have operated in an ethical manner and other entities believe that they have not been ethical in their operations. What SEA have shown is that unlike the hacktivist group Anonymous, SEA have focused only on a single political objective which has meant that their objectivity and motivation can be more closely questioned and their ethical beliefs consequently are much more difficult to determine.

The netnography aspect of the research study was a key factor. It allowed the researchers to develop a time frame of SEA activities, it allowed for an understanding of their actions and it allowed for an assessment against the SEA attack criteria. The netnography approach allowed for various online resources including online media and social media (including SEA own information channels) to be used for the study. This gave unique insights into the sorts of organisations that SEA attacks had focused upon and the type of online attacks undertaken. An interesting outcome of the netnography approach was that it highlighted that SEA had not always been ethical in their reporting of their activities. The researchers found examples of online attacks reported by SEA that they had undertaken that could not be verified by any other sources and there were therefore considered as being false claims.

Conclusion

As stated through the paper computer misuse is a global problem and groups such as SEA highlight the role that motivated hacking groups play in this global problem. The paper has successfully made use of the netnography approach to describe a complex online situation. The paper provides a detailed discussion of the SEA activities over an extended period of time and a discussion relating to the ethical stance of SEA.

Ethics is an extremely important component of cyber security, but the problem is that cyber security tends to concentrate on internal processes of access and amendment rights. The problem is that ethics influences the behaviour of individuals, whether the individual is trying to protect systems or attack systems.

As the start of March 2016, a military truce has taken place in Syria and peace talks have started (BBC, 2016). These developments will have a major impact on SEA and their future activities and hopefully bring peace to Syria.

Note

1. Available at: www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?_r=0l

References

Adams, J. (2013), *Decriminalising Hacktivism: Finding Space for Free Speech Protests on the Internet*, The George Washington University Law School, Washington, DC.

Al-Rawi, A.K. (2014), "Cyber warriors in the middle east: the case of the Syrian Electronic Army", *Public Relations Review*, Vol. 40 No. 3, pp. 420-428.

BBC (2016), "Syria conflict: Truce 'boosts peace talks', leaders agree", available at: www.bbc.com/news/world-middle-east-35727667 (accessed 3 March 2016).

Benkler, Y. (2012), "Hacks of valor: why Anonymous is not a threat to National Security", *Foreign Affairs*, 4th April, available at: www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of-valor?page=show (accessed 16 September 2015).

Bryan-Low, C. and Gorman, S. (2011), "Inside the Anonymous army of 'Hacktivist' attackers", *Wall Street Journal*, 23rd June, available at: http://online.wsj.com/news/articles/SB10001424052702304887904576399871831156018?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304887904576399871831156018.html (accessed 16 September 2015).

Conway, M. (2007), "Cyber Terrorism: hype and reality", in Armistead, L. (Ed.), *Information Warfare: Separating Hype from Reality*, Potomac Books, Washington, DC, pp. 73-93.

D'Amico, M.L. (1999), "Hackers spar over cyber war on Iraq, China", *CNN*, 13th January, available at: http://edition.cnn.com/TECH/computing/9901/13/cyberwar.idg/ (accessed 16 September 2015).

Denning, D.E. (2001), "Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy", in Arquilla, J. and Ronfeldt, D. (Eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Rand Corporation, California, pp. 239-288.

Facebook (2015), "Interest page: Syrian electronic army", available at: www.facebook.com/pages/Syrian-Electronic-Army/321083528028239# (accessed 16 September).

Hall, B.L., Clover, D.E., Crowther, J. and Scandrett, E. (2013), *Learning and Education for A Better World: The Role of Social Movements, Vol. 10 of International Issues in Adult Education*, Springer, New York, NY.

Hanna, K. (2013), "Wanking anonymously: the rise of hacktivism", *The Critic*, No. 19, 11 August, available at: www.critic.co.nz/features/article/3248/wanking-anonymously-the-rise-of-hacktivism (accessed 16 September 2015).

Held, W.V. (2012), "Hacktivism: an analysis of the motive to disseminate confidential information", Unpublished master dissertation, TX State University, TX.

Hwang, T. (2010), "WikiLeaks and the internet's long war", *The Washington Post*, Washington, 12 December, available at: www.washingtonpost.com/wp-dyn/content/article/2010/12/10/AR2010121002604.html (accessed 16 September 2015).

iGmena (2014), "Syrian electronic army a new emerging phenomenon", iGmena (internet Governance middle east and north Africa), available at: http://igmena.org/Syrian-Electronic-Army-a-new-emerging-phenomenon (accessed 16 September 2015).

Kozinets, R. (2002), "The field behind the screen: using netnography for marketing research in online communities", *Journal of Marketing Research*, Vol. 39 No. 1, pp. 61-72.

Kozinets, R. (2010), *Netnography: Doing Ethnographic Research Online*, SAGE Publications, New York, NY.

Levy, S. (1984), *Hackers: Heroes of the Computer Revolution*, Anchor Press, Norwell.

Leyden, J. (2013), "Syrian electronic army hacks US marines, asks 'bros' to fight on its side", *The Register*, 3 September, retrieved 14 June, available at: www.theregister.co.uk/2013/09/03/sea_hits_marines (accessed 16 September 2015).

Li, X. (2013), "Hacktivism and the first amendment: drawing the line between cyber protests and crime", *Harvard Journal of Law and Technology*, Vol. 27 No. 2, pp. 301-330.

NATO Review Magazine (2013), "The history of cyber attacks – a timeline", *NATO Review Magazine*, retrieved 16 June 2014, available at: www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm (accessed 16 September 2015).

Peters, J. (2013), "Is 2013 the biggest year ever for hacktivism", December, available at: www.hacksurfer.com/articles/is-2013-the-biggest-year-ever-for-hacktivism (accessed 16 September 2015).

Sterling, B. (1993), *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Mass Market Paperback, New York, NY.

Sterner, E. (2011), "Retaliatory deterrence in cyberspace", *Strategic Studies Quarterly*, Vol. 5 No. 1, pp. 62-80, Air University Press, Maxwell.

Syrian Electronic Army (2015), "Syrian electronic army Twitter account", available at: https://twitter.com/official_sea16 (accessed 16 September 2015).

Taddeo, M. (2012), "Information warfare: a philosophical perspective", *Philosophy & Technology*, Vol. 25 No. 1, pp. 105-120.

Tavani, H.T. (2005), "The impact of the internet on our moral condition: do we need a new framework of ethics?", in Cavalier, R. (Ed.), *The Impact of The Internet On our Moral Lives*, Suny Press, Albany, pp. 215-237.

Turner, R. (2014), "Tackling the DDoS threat to banking in 2014", *Ovum*, 27 January, retrieved 10 June, available at: www.akamai.com/dl/akamai/ovum-tackling-ddos-threat-in-banking.pdf?campaign_id=F-MC-23039 (accessed 16 September 2015).

Walker, T. (2013), "Hacked off: what happened when the Syrian electronic army attempted a cyber attack on The Independent?", available at: www.independent.co.uk/news/uk/home-news/hacked-off-what-happened-when-the-syrian-electronic-army-attempted-a-cyber-attack-on-the-independent-8874891.html (accessed 16 September 2015).

Warren, M.J. and Hutchinson, W. (2003), "Australian hackers ethics", *Australian Journal of Information Systems*, Vol. 10 No. 2, pp. 151-156.

Weimann, G. (2005), "Cyberterrorism: the sum of all fears", *Studies in Conflict and Terrorism*, Vol. 28 No. 2, pp. 129-149.

Corresponding author
Matthew Warren can be contacted at: matthew.warren@deakin.edu.au