The Centre for the Study of Terrorism and Political Violence
Journal of Terrorism Research

Articles

'Close enough' – The link between the Syrian Electronic Army and the Bashar al-Assad regime, and implications for the future development of nation-state cyber counter-insurgency strategies

by Stewart K Bertram

Abstract

The purpose of this paper is to examine the formality of the relationship, or lack thereof, between the Bashar Al Assad regime in Syria and the Syrian Electronic Army (SEA). The paper uses a qualitative approach to the research, with an adapted form of Social Network Analysis used to analyse the connections within the data. The core conclusion of the research is that a relationship exists between Assad and the SEA, which is close enough to assist Assad in foreign policy goals, while distant enough to provide plausible deniability for the regime. The paper defines this relationship as 'close enough.'

Keywords: *cyber counter-insurgency; Syria; Assad; proxy force; hacktivism; computer hacking*

In 2016 the United States (US) Federal Bureau of Investigation (FBI) added two alleged members of the Syrian Electronic Army (SEA) computer hacker group to its cyber 'most wanted' (FBI News, 2016) list. The FBI justified the listing by stating that the two individuals had, as part of their involvement in the SEA, through their actions *"…provide*[d] *support to the Assad regime"* and, in so doing, *"sought to harm the economic and national security of the United States in the name of Syria"*. This event was highly significant for a number of reasons; firstly, the two SEA members were the first politically motivated hackers (hacktivists) to be named on the most-wanted list, and secondly, the US legal charges and FBI manhunt signalled the tangible international and political impact that the SEA had achieved through its activities.

The actions of the SEA have doubtlessly been provocative; however, many questions remain unanswered. One concerns the formality of the relationship between the SEA and the Assad regime. Varying opinions have developed, ranging from labelling the group as an outright proxy force for Assad (Al-Rawi, *et al* 2014) to labelling its members as little more than amateurs and an adjunct to the wider Syrian conflict (Motherboard, 2013).

Although this paper deals directly with the evidence that attributes the SEA to the Assad regime, the research takes a perspective that is different from the usual 'proxy or not?' debate, rejecting this binary approach for a more suitable investigation of the data. The paper outlines the strategic logic behind the SEA as a group distant enough from the Assad regime to provide plausible deniability, but close enough to interpret and meaningfully pursue state political goals in cyberspace. This relationship is the proposed as a 'close enough' relationship between a non-state cyber group and a state authority. From this base the paper considers the strategic advantage to both state and group when engaged in a cyber counter-insurgency (cyber-COIN) style of conflict.

The remainder of the paper comprises a review of insurgency/COIN studies and US military thinking on aspects of cyber warfare, followed by a brief explanation of the qualitative research method. The core of the paper is an in-depth analysis of a previously overlooked aspect of the available data that illustrates the close enough nature of the relationship between the SEA and the Assad regime. The paper concludes with an analysis that fuses the conclusions of the previous sections with wider COIN theory.

Literature

Conflict-driven human interaction within cyberspace has been a growing focus of academic study for a number of years. Early investigations into cyber intrusions of such victims as the Office of His Holiness the Dalai Lama in 2007 (Information Warfare Monitor 2010), and theorization about cyber attacker methodologies, (Caltagiron *et al*, 2016 and Hutchins *et al*, 2016) paved the way for an entire sub-section of the cyber security industry. They also led to serious academic study into the phenomenon of computer hacking.

Contiguous to this development within the private sector and academic sphere, the US military, led predominantly by the US Air Force, theorized about the shape of military operations in cyberspace. A major output of this process was the recognition of cyberspace as the 'the fifth domain' (Robert, 1996) of military operations. This categorisation heralded the development of sub-categories of military operations in cyberspace, such as Computer Network Operations (CNO), Computer Network Attacks (CNA) and Computer Network Defence (CND). Each of these classifications has unique characteristics, and from this observation it is obvious that there are differing conceptualisations of the forms that state power projection into cyberspace can take. Operations range from high-tech, ultra-covert cyber espionage (the so-called Advanced Persistent Threat) to much less technical but much more public displays of power (Russia's so-called web brigades, Веб-бригады, or the 'Troll Armies', for example (Polyanskaya *et al*, 2003)).

Within this scale of state capabilities, at the technical 'softer' social media enabled pole of the scale, there is often the observable social dynamic of two opposing groups competing to shape the behaviour and actions of a target audience. The classic actor relations thus emerge among insurgent, counter-insurgent and the target audience they are attempting to influence (Taber, 1965).

Within this actor tri-graph the idea of a *cyber insurgency* as a stand-alone concept is observable developing within the post-9/11 US military as early as 2011 (Hagestad, 2011 and 2013). The core idea seeming to underpin this concept is that COIN warfare in physical space did not just bare a passing resemble to some emergent conflicts in cyberspace; instead, that COIN doctrine could be directly applied to the fifth domain because the doctrinal axioms underpinning cyber and physical insurgencies are one and the same.

Although still awaiting enshrinement in official military doctrine, the concept of 'cyber-COIN' was effectively recognised as a valid concept by the US military in 2015 with Duggan's work (Duggan, 2015). He proposed the idea of 'Counternetwork COIN' and defined the tactic as employing "*nontechnical attacks against people to manipulate their perceptions, behaviors, and actions*" (Duggan, 2015: 50). The existence of such a thing as cyber-COIN is supported by scholars such as Rid, who commented: "*…the new Web, in an abstract but highly relevant way, resembles — and inadvertently mimics — the principles of subversion and irregular warfare*" (Rid *et al*, 2009: 2).

Turning to the Syrian conflict, a number of scholars have examined the cyber element through the insurgent/

COIN/target audience framework that underpins cyber-COIN, without explicit reference to the concept. Very few of these papers critically examine the nature of the relationship between the Assad regime and the SEA, thereby undermining much of their arguments with assumptions about the nature of the relationship. Shehabat's work (Shehabat, 2011) categorises all actors within the Syrian conflict into three broad categories: '[Syrian] State versus foreign organizations,' '[Syrian] State versus individual' and 'foreign organizations versus [Syrian] State.' However, this omits the 'non-state pro-Assad actor' category, within which the SEA may conceivably fit.

Other scholars are more deterministic; some have said the SEA is an Assad (Khamis *et al* 2014 and Zambelis, 2012)–or even Iranian (Duggan, 2015) state-backed group, and some have simply refused to address the nature of the relationship entirely. A case of this is in one of the few notable quantitative studies of the SEA. Callaghan, *et al* (2014) examines how the group sits within the wider context of the social network of all groups active in the conflict. This study confirms the presentation of the SEA as a leader within the pro-Assad faction of the cyber conflict, but carefully avoids developing an opinion on the relationship between the group and the state. Kan is one of the few to muse on the importance of the subject, commenting: *"Who exactly is the Syrian Electronic Army? Is it a group of a state-sponsored "patriotic hackers," an unaffiliated association, a loose assemblage of individuals sympathetic to the regime of Bashar Assad, or some combination of each?"* (Kan, 2013: 113)

To ignore the specific aspects of the Assad/ SEA relationship is dangerous, given both the rising importance that cyber conflict is playing in international relations, and the nuanced complexities of the relationship between a state authority and proxy force that have been shown to exist outside of a cyber context through studies of groups such as the US Minutemen movement (Shapira, 2013).

When attempting to understand the importance and complexity of the issues of the state/non-state proxy actor relationship an unusual but potentially useful case study has arisen with the context of the relationship between the famous US actor Steven Seagal and Russian Federation president Vladimir Putin. After an extended friendship, Putin recently bestowed Russian citizenship upon Seagal, commenting that the gesture *"might be a sign of the gradual normalization of relations between our countries"* (Roth, 2016). His comment shows that his relationship with Seagal can be seen (by Putin, at least) as having some influence on the relationship between the US and Russia. Although Seagal's actions may mirror the warmer sentiment and conciliatory air towards Russia coming from US President Donald Trump (Rozsa, 2016), it is a mistake to naturally assume that Seagal is, by default, a legitimised and official arm of US foreign policy. As curious as the case study is, the dynamics between state and proxy force that the case highlights are as applicable to the relationship between the SEA and the Assad regime. It is this dynamic, seated within a cyber-COIN framework, which the remainder of this paper examines.

Method

The core topic of study for this paper is the nature of the relationship between the SEA — as a group and as individual members — and the Assad regime. By necessity, addressing this issue has required an attempted attribution of SEA activity to the Assad regime. Although there are suggested frameworks for actor attribution within a cyber context (Rid *et al*, 2014), there is scant publically available information on the SEA of the type required to apply such models. Given that this data is unlikely to become available to researchers in the near future, a broad approach to gathering qualitative data from unconventional sources has been used for this research. Annex A of this document provides an overview of the main data source categories used.

The researcher acknowledges that most data presented in this paper is circumstantial and susceptible to error. The justification for the approach to data collection is that no single publically available data source provides a foundation to support the theoretical goals of the research. In defence of this position, most, if not all, academic and cyber security industry publications on the SEA are based on similar data sources, often without acknowledgment of the potential risks of using them.

Steps taken to mitigate these limitations include:

- The caveat that all source data included in the paper, although critically assessed to the best of the researcher's capabilities, was ultimately accepted in good faith; it is assumed that sources have not actively tried to deceive or present falsified data.
- All results are transparently presented, with extensive footnotes, to allow the reader to accurately source the data and reconstruct the analysis used within the report.
- In an attempt to manage analyst bias Heuer's *Analysis of Competing Hypotheses* (ACH) method (Heuer, 1999), along with the weighted scoring method implemented within the Parc ACH software (ACH2.0.5 Download Page, 2016) was used to analyse five separate hypotheses around the relationship between the Assad state and the SEA. These hypothesis and results are presented in Annex B, along with the source of each item of data.

The collected data has been analysed in several ways, including a timeline analysis of the SEA's activities (Annex C) and a modified form of Social Network Analysis used to assess the SEA's email links to the regime. The specific modification was for the graphs to show only communication from a single individual to a wider network, as opposed to direct communication within a network. Where necessary, a native bilingual Arabic/ English speaker has been employed to verify translated text.

Attributing the SEA to the Assad regime

Although it is certain that the SEA is staunchly pro-Assad, the formality of its relationship to the regime remains deeply ambiguous. Even the SEA itself, in its early form, seemed unsure of its position on this issue; the group claimed to be an official arm of the pro-Assad Syrian state in the very first iteration of Syrian-es.com (IntelCrawler, 2014), only to retract the statement a short time later (IntelCrawler, 2014). This on-again/ off-again nature of the SEA's approach to the relationship typified much of the group's early communications; however, in later years the group has adopted a policy of routinely denying any formal connection to the regime (Keys, 2013 and Katerji, 2013 and Ferran, 2013). Of course the SEA's public denial of a connection to the regime does not automatically separate state and group, especially given the SEA's involvement in activities that it defines as 'counter terrorism' (Cameron *et al*, 2013).

An inadvertent attempt to clarify the Assad/ SEA relationship lies within thewithin wording of the FBI's 'cyber most wanted' list and the varying ways relationships are described, when comparing the listing of the SEA members and a separate group of Iranian hackers. The carefully worded listing for the SEA describes its actions as '*in* support of the Syrian regime' (FBI, 2016a, 2016b,) rather than hacks *on behalf* of the Syrian regime (FBI, 2016c). This nuanced use of language by the FBI is deliberate, as demonstrated by the more explicit language it uses to link official organisations of the Iranian state to a separate group of cyber activists on the list (FBI, 2016c). The difference in wording strongly suggests that the US government has, at least, recognised the ambiguous nature of the relationship between the Assad regime and the SEA.

Even a cursory examination of both the way the group describes itself and the way it is described by third parties, shows that a deeper examination of the available data is necessary when considering an attribution of the SEA to the Assad regime.

The Syrian Computer Society connection

Possibly the next most common port of call after the SEA's own statements regarding their relationship to the Assad regime, comes from Bashar al-Assad's former status as the head of the Syrian Computer Society (SCS). Although rarely explicitly stated, the intimation is that Assad is somehow naturally predicated to support groups like the SEA, due to his former post (Giles, 2012). Further examples of this logic comes from Noman, who, when asked about the relationship between the Assad regime and the SEA, stated:

"*What we know is that* [the SEA's former] *domain name was registered by the Syrian Computer Society. We looked into the Syrian Computer Society and discovered that it was headed by* [Bashar] *al-Assad in the 1990s… It's hosted on the network of the Syrian government.*"(Bea quoting Noman, 2013)

Although the above statement is built from facts, the presentation of these facts is misleading. Noman relies on implication of their potential meaning over critical analysis of their actual meaning. Others seem content with the implications of a connection between the SEA and the SCS (Grohe, 2015) while others such as Shehabat, go further and conclude that the SEA is an arm of the "*embattled regime's intelligence service*" (Shehabat, 2011: 6), by incorrectly asserting that the "Mukhabarat" (Syrian military intelligence) owns the SCS (Shehabat, 2011) and that hence the SEA is in effect an adjunct government entity due to its connection to the SCS.

A possibly more meaningful analysis moves away from Assad's relationship to the SCS and what it may imply about the SEA, while still acknowledging the importance of the role of the SCS as the sole state-backed provider of Syrian web domain hosting services. Given that the SEA's main website (http://www.syrian-es.com/ or "Syrian-es.com", which is currently offline) is hosted by SCS-NET, the arm of the SCS tasked with internet service provision (ISP) and all "es" domain name registration in Syria, the Syrian state appears to be providing, in effect, a cyber safe haven for the SEA.

The SCS is a pro-Assad arm of the Syrian government, and the group and all of its ISP infrastructure have been controlled by pro-Assad forces during the conflict. Given these facts, the uninterrupted presence of content on Syrian-es.com for at least three years suggests a relationship that goes beyond mere acquiescence of the state towards the SEA; it suggests material support of the SEA from the state. The most obvious counter argument to this assertion is that that the regime is simply not aware of the existence of Syrian-es.com, or even of the SEA. This is unlikely, given the early exposure the SEA received in the domestic pro-Assad media (Noman, 2016) and a speech Assad gave in 2011(O'Brien, 2011). In that speech he stressed the validity of cyberspace activity in the wider context of the Syrian conflict, and came close to directly name-checking the SEA.

A final observation that supports the theory that the Assad regime is deliberately choosing to allow the SEA to operate out of a digital safe harbour is that the regime, as a body, has been extremely successful in regulating internet content in Syria, periodically blocking access to such services as YouTube, Twitter and Facebook (Shehabat, 2011), and routinely removing opposition websites from the es space. This demonstrates a granular awareness of the content of the es space by the Assad regime, and in turn implies a deliberate decision to not remove the SEA content.

Where does this observation leave the Assad regime with regard to its accountability for the activities of the

SEA? Returning to the Steven Seagal-Vladimir Putin case study, while there is no evidence of a US authority actively endorsing Seagal's international relations efforts, there is equally no evidence of the US authority making attempts to prevent them. This highlights an important concept: that a nation state's lack of restraint of groups/individuals claiming to represent its interests is as important as positive reinforcement of them. In plain terms, in certain situations silence can speak volumes. What differentiates the Seagal-US and Assad-SEA cases is that the SEA is engaged in overtly criminal activities in the name of the state. Actions that when directed at the Assad regime, the regime is quick to stamp out. These factors further imply acquiescence on the part of the Assad regime towards the SEA

Although the persistence of Syrian-es.com does not go so far as to prove the SEA is, as some have claimed, a "*state-supervised*" (Gallagher, 2013) organisation, it does show that the Assad regime is, at the very least, adopting a highly biased 'blind-eye policy' towards the group.

Other connections

The insight that can be drawn from the Assad regime's approach to the SEA website is that the group is closer to the regime than the standard Internet user; however, there are other pieces of data available that may add clarity to this assessment.

A potentially useful example arose in July 2012 with the WikiLeaks release of the *Syria Files* (WikiLeaks, 2012), a trove of email messages stolen by hackers from multiple members of the pro-Assad regime. It contained more than two million messages spanning August 2006 to March 2012. Given the volume of communication, the date range, the representation of prominent regime figures in the files, and the Assad regime's previously demonstrated lack of discretion in regards to secure communication, this data is an obvious source to examine for evidence of a more tangible SEA connection to the regime.

One such connection within the Syria Files data set is apparent between the SEA's Tiger persona and elements of the Syrian authority (although the Tiger persona is not named within the FBI indictment but appears to conduct support functions, such as malware testing and infrastructure maintenance). With two occurrences of messages involving the tiger.tiger248@gmail.com ('tiger.tiger248'), being evident within the files. This is significant as the tiger.tiger248 email address has been linked to the Tiger persona and was left as part of the SEA's 'calling card' in previous website defacements claimed by the group (the most prominent of which was the 29 July 2013 defacement of the Thomson Reuters Twitter account.)

Various commentary on the SEA has identified the presence of the tiger.tiger248 address within the Syria Files, and speculated that it may link the SEA to the Assad regime (IntelCrawler, 2014). However, this assessment accepts, at face value, the WikiLeaks claim suggested by the data set's presentation: that all the email addresses in the Syria Files are directly related to the pro-Assad Syrian regime.

Upon deeper investigation, it becomes apparent that tiger.tiger248 was the addressee on two messages, both from gk005@hotmail.com ('gk005'). The first message commented on the mostly non-violent nature of anti-government protests (WikiLeaks, 2012a). The other detailed the Assad regime's attempts to find a non-violent solution to the conflict. Although the intended meaning of the messages is difficult to discern without further context, they appear to be relatively bland, propaganda-style press releases aimed at supporters of the Assad side of the conflict.

The gk005 address has been attributed by the researcher to an individual named Ghaleb Kandil (he cites it as his contact address on Facebook (Kandil, 2016)). Kandil is a Lebanese mainstream journalist (translated career biography included in Annex D) who has been responsible for a number of pro-Assad news reports since the start of the conflict. The WikiLeaks Syria Files database revealed seven messages from or to gk005, including the two sent to tiger.tiger248. Of the fifteen addressees included within the seven emails, only two appear to be obvious Syrian government email addresses. The others are webmail accounts, such as Gmail and Hotmail, which reduces their diagnostic value for attribution to the Syrian regime. The two Syrian government email addresses that gk005 had communicated with are profiled as follows.

- n.kabibo@mopa.gov.sy — gk005 only sent one message to this address, which was actually defunct when the message was sent, on 16 April 2011 (shown by an email delivery failure message dated 18 February 2010 (WikiLeaks, 2012b)) (WikiLeaks, 2012c). From the analysis of other messages from and to this address, the account appears to have belonged to a junior Ministry of Presidential Affairs official named Nizar Kabibo. Kabibo's job seems to have been coordinating visits by foreign journalists to Syria, as assessed from messages sent by such organisations as Sky News, which informed the recipient of upcoming foreign coverage of Syria and Assad (WikiLeaks, 2012d).
- minister@moi.gov.sy — gk005 sent five messages containing pro-Assad content, in a similar thematic vein to the messages sent to tiger.tiger248. This is most likely a generic Syrian Ministry of Interior address (possibly harvested from the contact form on the Syrian government home page (Syrian Ministry of Interior Home Page, 2016)) to which gk005 may have been sending pro-Assad news articles for comment.

Useful in further defining Kandil/gk005's relationship to the Assad regime is the analysis of a separate 2012 dump of Assad's personal email account (Booth *et al*, 2012). From this trove two individuals (Sheherazad Jaafari and Hadeel al-Al), sharing one email address (sam@alshahba), were identified as key personal advisers to Assad on mainstream media management and the regime's approach to social media. Within the Syria Files there are no examples of communication between the sam@alshahba address and either gk005 or tiger.tiger248. This further distances gk005 and the SEA from the core inner circle of the Assad regime.

A graphical representation of the relationship between the tiger.tiger248 address and the Syrian government address is shown in Figure 1, for clarity.

Image 1

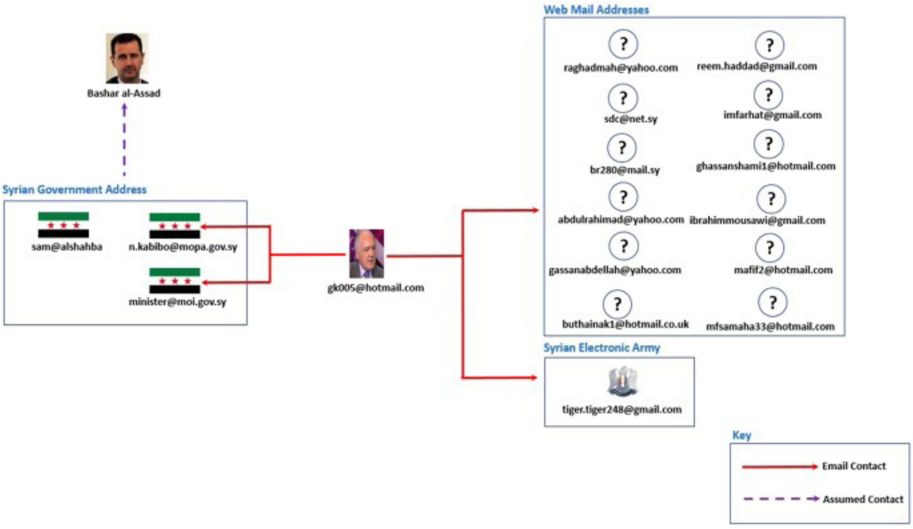

Figure 1: Communications from gk005@hotmail.com

The analysis presented in Figure 1 demonstrates that even a claim of loose association between the SEA and the Syrian authority is shaky, at best, if based solely on the presence of tiger.tiger248's email address in the Syrian Files. The most that can be claimed is a third degree of separation between the Tiger persona and a defined figure linked to the Assad regime, and even this is charitable — under some social network analysis frameworks, the fact that the n.kabibo@mopa.gov.sy address was defunct at the time of gk005's message would classify the relationship as having no connectivity value whatsoever (Figure 1 is intended to show communication attempts by gk500, rather than a bi-directional communication network).

Compounding the issue of the relevance of the gk005 persona is the very short date range the seven email messages cover; one was dated 16 April 2011 and the other six were sent from 5 to 14 July 2011. These observations regarding the tiger.tiger248 address, combined with the absence of any other address linked to the SEA in the Syria Files, are far from linking the SEA to the Assad regime. Instead, they place it on the very peripheries of the regime, and paint a partial picture of a group maintaining loose links to regime outliers.

This assessment stands in stark juxtaposition to the assessment around the Assad regime's indirect but overt support of the SEA through their inaction around the SEA's presence within the es web space, and paints the picture of a state backing a group but without apparently communicating with it. While it is possible that this communication between state and group is simply not observable, this is unlikely given how senior members of the Assad regime have shown to be communicating across the spectrum of the pro-Assad government apparatus in both the Syria Files and 2012 data leeks. Instead the researcher would propose that the evidence points to an alternative form of relationship between the SEA and the Assad regime.

Close Enough?

In the absence of a 'smoking gun' piece of evidence that conclusively links or fully separates the Assad regime and the SEA, a picture emerges of a loose connection between state and group, the 'close enough' relationship proposed by this paper. Within this relationship are strategic incentives for both parties to keep the SEA at a distance from the regime, preserving deniability, while keeping them closer than the average Syrian to maintain the group's acquiescence to Assad policy. When viewing the available data through this lens a more satisfying picture of state and group relationship emerges.

Indirect contact with the regime through individuals, such as Ghaleb Kandil/gk005, and pro-Assad media organisations, such as http://documents.sy/ (attributed by a 2014 data breach of the site), places the Tiger persona close enough to the regime to be cognisant of the desired direction of the pro-Assad media narrative. However, it maintains enough distance from core regime figures to preserve the regime's plausible deniability of SEA actions.

The trend set by the loose connection of the Tiger persona to the pro-Assad media appears not to be an anomaly and continues within examples of other SEA-attributed emails and their context in the Syria Files leaks. For example, the SaQeR.SyRia@gmail.com address left by the SEA on a defaced page of the French embassy in Damascus in 2011 (Information Warfare Monitor/OpenNet Initiative, 2016) appears in the Syria Files as a recipient of further media-style state communication (WikiLeaks, 2012e). When analysing the data collectively within the ACH methodology framework (Annex B), of the five hypothesis tested, the least disproved hypothesis with a score of -11.0 (the hypothesis closest to 0 is considered the least disproved) is that the *SEA is informally connected to the Assad regime through inadvertently generated connections.*

When an alternative to the concept of one-to-one relationships representing power is abandoned, then the SEA's status within a 'close enough' network becomes far more significant. The 'strength of weak ties' (Granovetter, 1973) theory would appear to underlie this 'close enough' nature of the SEA, as even loosely connected networks can be extremely powerful under certain circumstances. This is practically illustrated through the expansion of the gk005 network shown in Figure 1, with further data drawn from the Syria Files and a previously insignificant email address (new data shown in green in Figure 2 below).

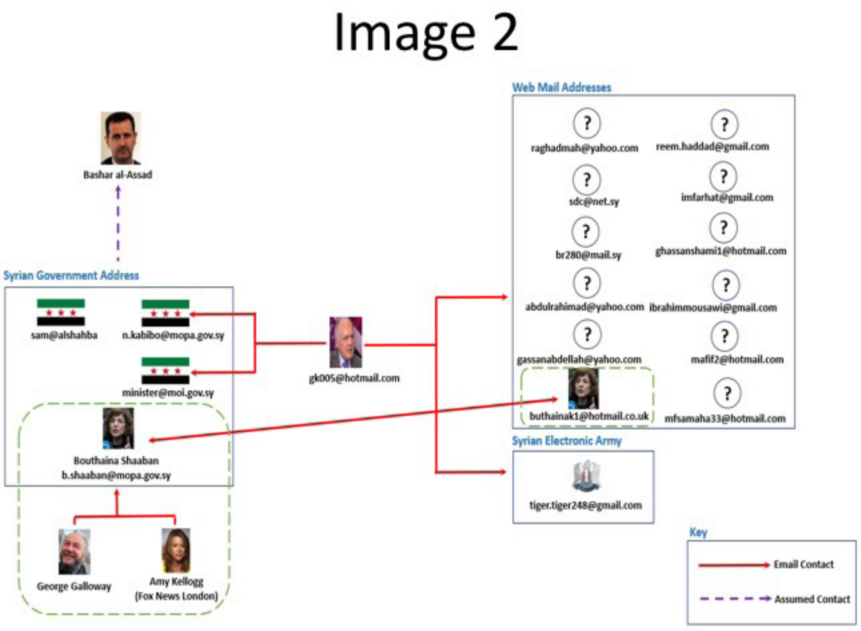

Figure 2: Expanded communication network of gk005@gmail.com (new elements highlighted in green)

The previously unattributed buthainak1@hotmail.co.uk address tracks back to Bouthaina Shaaban (via b.shaaban@mopa.gov.sy). Shaaban is the current most-senior media advisor to Assad and a senior political figure in her own right within the regime. Closer analysis of Shaaban's emails shows direct contact with senior Western media personalities and political figures, such as Amy Kellogg from Fox News London (WikiLeaks, 2012f) and former UK member of parliament George Galloway (Ravid, 2012).

This new data still separates the SEA from Assad and the regime; however, the incorporation of an individual like Shaaban now places members of the SEA in direct contact with a significant regime interlocutor, two degrees of separation from a major regime figure and three degrees from a major, internationally recognised Western political figure. While there is still no evidence of direct contact between Shaaban or Galloway and the SEA, the network fragment depicted in Figure 2 hints at a potentially powerful social network that could be easily leveraged by the Syrian State.

The strategic appeal of 'close enough' for a cyber-COIN force

It is unknown whether the creation of a 'close enough' relationship between the SEA and the Assad state is the result of a deliberate choices by either party, or even whether either group is aware of the dynamics of the relationship. What can be assessed, however, are the benefits the relationship bring for both parties within the SEA-adopted role as a cyber-COIN force for the Assad regime.

The distance between the Assad regime and the SEA is obviously appealing from Assad's perspective, through the classic benefits brought by a state utilizing a proxy force (Mumford, 2013), but the relationship also benefits the SEA. As the group is not technically an official organ of the Assad state, it can engage in activities that would be prohibited were the relationship more formal. An example of this power is the group's mobilisation of a pan-Arabic diaspora (the most prominent example being the close correlation of the target set pursued by both the SEA and various Iranian hacking groups circa 2011 (Information Warfare Monitor/OpenNet Initiative, 2016). Another example is found in temporary alliances with hacker groups that have vehemently opposed the Assad regime (e.g. the SEA-Anonymous 'team up' in 2013 and the joint targeting of the Turkish government networks (Russia Today, 2013)).

Additionally, ideological flexibility allows the SEA to present messages with an air of quasi-legitimacy that would appeal to the core Assad opposition — something official organs of the Assad regime could not credibly do. This allows the SEA (and, by default, the Assad regime) to challenge what Rid terms the 'taboo' (Rid, 2009) of the COIN force: appearing to give ground on the core issue of the insurgency. The SEA is left free to intimate changes and concessions that could rob the Assad opposition of online support, while the Assad regime retains the ability to later deny any concessions intimated by the SEA due to that lack of a formalised relationship.

Through the wider lens of COIN theory, the SEA's 'close enough' nature gives the group the powerful ability to invert aspects of the insurgent/COIN dynamic, such as Rid's 'taboo' factor and a number of the asymmetries between insurgency and COIN observed by Galula (Galula, 1964). Such factors as the COIN force being bound by truth, and anonymity harming the COIN cause, become flexible in the hands of the SEA. Moreover, most importantly for the Assad cause, the SEA inverts Rid's third summation of Galula's asymmetries — that "*traditionally within the media sphere, the insurgent has the initiative while the counterinsurgent reacts*" (Rid *et al*, 2009; introduction Xi). This is hugely important in a conflict with a significant cyberspace component, owing to the naturally weaker position the state finds itself in within a cyber-insurgency context. As Rid comments, "*on balance, the new media environment tends to favour the* *irregular forces within an insurgency-style conflict.*" (Rid *et al*, 2009: 2) He adds, *"the unintended consequences for armed conflict is that non-state insurgencies benefit far more from the new media than do government and counter insurgencies.*" (Rid *et al*, 2009: 14). The 'close enough' relationship allows the SEA to challenge these imbalances, regardless of the formality of the relationship it has with the state.

Conclusion

Whether the creation of the SEA is the result of a deliberate covert operation on the part of a state organisation or merely a happy coincidence for the regime, the latitude that the Assad regime has undoubtedly given to the SEA has allowed the group to deliver what some have assessed as "*the most sophisticated response* [from a state] *to* [the] *online activism of the Arab Spring*" (Fisher *et al*, 2011).

With such heady praise for the SEA's achievements, the lack of definition of the true nature of the relationship between the Assad regime and the group is unsatisfactory. This paper has examined the available data on the SEA and the wider digital aspect of the Syrian conflict in an effort to fill this gap.

What the researcher found was that the available data neither conclusively connected the Assad regime to the SEA, nor did it equivocally separate them. The final conclusion of the research is that a deterministic piece of data that would resolve this impasse was not found because it does not exist. Moreover, the true nature of the relationship between state and group lies somewhere between the poles of stated-backed and autonomous activist group. Other researchers have observed that the Assad state created an environment for the SEA to succeed (Syrian Freedom, 2012), but it is this paper's unique contention that this 'close enough' connection creates a virtues circle between state and group irrespective of the formality of the relationship. Additionally, the paper highlights the strategic advantages to both parties of a 'close enough' relationship within a cyber-COIN context, thus adding much-needed animation to the often theoretically thin concept of cyber-COIN.

The future implications for this research are significant, given the pivotal role that cyberspace appears to have played not just in the Syrian conflict and the wider Arab Spring, but in conflicts such as the one currently ongoing in the Ukraine. While researchers are now understanding the role of the cyber insurgent, an examination of the nation state's response to cyber insurgency is hugely under-addressed within the literature. The need for this study comes from an observation made by Galula (1964) eruditely pointing out, that there is not a single rule set for revolutionary warfare. Instead there is the set of rules and principles that guides the revolutionary, and a separate set that guides the counter-revolutionary and only through understanding both can we hope to understand the details of a conflict.

About the author

Stewart Bertram *is a talented and experienced intelligence and security professional who combines nearly a decade of expertise with relevant academic qualifications. Grounded solidly in a background of computing and social science, Stewart presents a professional customer facing offering, that mixes technical skill with a transparent and easily accessible research methodology.*

Bibliography

ACH2.0.5 Download Page, available online as of 1 June 2016 from: http://www2.parc.com/istl/projects/ach/ach.html

Al-Rawi, Ahmed K, (2014), *Cyber warriors in the Middle East: The case of the Syrian Electronic Army,* available online as of 8 December 2016 from: http://www.sciencedirect.com/science/article/pii/S0363811114000824

Booth, R, Mahmood, M and Harding, L (2012), *Exclusive: Secret Assad Emails Lift Lid on Life of Leader's Inner Circle,* available as of 2 August 2016 from: https://www.theguardian.com/world/2012/mar/14/assad-emails-lift-lid-inner-circle

Bea, F quoting Noman, H (2013), *Can the Syrian Electronic Army Weaponized Twitter to Topple Western Media?,* Digital Trends, available as of 2 August 2016 from: http://www.digitaltrends.com/social-media/syrian-electronic-army-and-the-shadow/

Cameron, D and Katerji, O (2013), 'The Syrian Electronic Army Talks About Tuesday's Hack', *Vice*, available as of 2 August 2016 from: http://www.vice.com/read/the-syrian-electronic-army-talks-about-yesterdays-hacks

Caltagirone, S, Pendergast, A and Betz, C, *The Diamond Model of Intrusion Analysis*, available as of 2 August 2016 from: https://www.threatconnect.com/wp-content/uploads/ThreatConnect-The-Diamond-Model-of-Intrusion-Analysis.pdf

Duggan, PD, (2015), *Strategic Development of Special Warfare in Cyberspace*, National Defense University Press, available as of 8 December 2016 from: http://ndupress.ndu.edu/Media/News/News-Article-View/Article/621123/strategic-development-of-special-warfare-in-cyberspace/

Derek O'Callaghan, D,Prucha, N, Greene, Conway, M, Carthy, J, Cunningham, A, (2014), *Online Social Media in the Syria Conflict: Encompassing the Extremes and the In-Between,* available as of 8 August 2016 from: https://arxiv.org/pdf/1401.7535.pdf

FBI News (2016), *Syrian Cyber Hackers Charged Two From 'Syrian Electronic Army' Added to Cyber's Most Wanted,* available online as of 2 August 2016 from: https://www.fbi.gov/news/stories/two-from-syrian-electronic-army-added-to-cybers-most-wanted

FBI, (2016a) *Firas Dardar*, available as of 2 August 2016 from: https://www.fbi.gov/wanted/cyber/firas-dardar

FBI, (2016b) *Ahmed Al Agha*, available as of 2 August 2016 from: https://www.fbi.gov/wanted/cyber/ahmed-al-agha

FBI, (2016c) *Sina-Keissar*, available as of 2 August 2016 from: https://www.fbi.gov/wanted/cyber/sina-keissar

Ferran, L (2013), *Interview with Alleged Member of Syrian Electronic Army,* ABC News, available as of 2 August 2016 from: http://abcnews.go.com/blogs/headlines/2013/08/interview-with-alleged-member-of-syrian-electronic-army/

Fisher, M and Keller, J (2011), 'Syria's Digital Counter-Revolutionaries', *The Atlantic*, available as of 2 August 2016 from: http://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/

Gallagher, S (2013), 'Network Solutions Seizes Over 700 Domains Registered to Syrians', *Ars Technica*, available online as of 2 August 2016 from: http://arstechnica.com/tech-policy/2013/05/network-solutions-seized-over-700-domains-registered-to-syrians/

Giles, J, Mark, P (2012), *Assad masses Syrian cyber army in online crackdown*, New Scientist: available as of 2 August 2016 from: https://www.newscientist.com/article/dn21506-assad-masses-syrian-cyber-army-in-online-crackdown/

Grohe, E (2015), *The Cyber Dimensions of the Syrian Civil War. Implications for Future Conflict,* John Hopkins University Physics Laboratory, available as of 2 December 2016 from: http://www.jhuapl.edu/ourwork/nsa/papers/TheCyberDimensionsoftheSyrianCivilWar.pdf

Galula, D (1964), *Counter-Insurgency Warfare Theory and Practice,* available as of 2 August 2016 from: http://louisville.edu/armyrotc/files/Galula%20David%20-%20Counterinsurgency%20Warfare.pdf

Granovetter, M S (1973), 'The Strength of Weak Ties', *American Journal of Sociology*, Vol 78, Issue 6 (May 1973), pages 1360-1380, available as of 2 August 2016 from: https://sociology.stanford.edu/sites/default/files/publications/the_strength_of_weak_ties_and_exch_w-gans.pdf

Hutchins, E, Cloppert, M, and Amin, R, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,* available as of 2 August 2016 from: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Hagestad, W. 'Mandarin Chinese as the Ultimate Form of Cryptography', *Conference Proceedings: Cyber Defense & Network Security 2011,* and updated: Hagestad, W, 'Comparative Study: Iran, Russia & PRC Cyber War', *Conference Proceedings: RSA Europe 2013*, presentation available as of 2 August 2016 from: https://www.rsaconference.com/writable/presentations/file_upload/hta-w01-comparative-study-iran-russia-prc-cyber-war_copy1.pdf

Heuer, R (1999), *"Chapter 8: Analysis of Competing Hypotheses",* Psychology of Intelligence Analysis, Center for the Study of Intelligence, Central Intelligence Agency, available as of 17 August 2016 from: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf

Information Warfare Monitor (2010), *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, available as of 2 August 2016 from: http://www.nartv.org/mirror/shadows-in-the-cloud.pdf

Information Warfare Monitor/OpenNet Initiative (2016), *Syrian Electronic Army: Disruptive Attacks and Hyped Targets,* available as of 2 August 2016 from: https://opennet.net/syrian-electronic-army-disruptive-attacks-and-hyped-targets

IntelCrawler (2014), *Syrian Electronic Army – Hactivision to Cyber espionage?,* available as of 2 August 2016 from: http://www.slideshare.net/RDSWEB/intel-crawler

Kandil, G Facebook page, available as of 2 August 2016 from: https://www.facebook.com/Ghaleb-kandil-199503680115989/info?tab=page_info

Kan, PR, (2013), *Cyberwar to Wikiwar: Battles for Cyberspace*, Examining Warfare In Wi-Fi, available as of 8 December 2016 from: http://www.dtic.mil/get-tr-doc/pdf?Location=U2&doc=GetTRDoc.pdf&AD=ADA598606

Khamis, S, Gold PB, Vaughn, K, (2014), *Beyond Egypt's "Facebook Revolution" and Syria's "YouTube Uprising:" Comparing Political Contexts, Actors and Communication Strategies,* University of Maryland, College Par, available as of 8 December 2016 from: https://www.researchgate.net/profile/Paul_Gold2/publication/267383659_Beyond_Egypt%27s_Facebook_Revolution_and_Syria%27s_YouTube_Uprising_Comparing_Political_Contexts_Actors_and_Communication_Strategies/links/546ce4bd0cf2a7492c55ad75.pdf

Keys, M (2013), *A Live Conversation with the Syrian Electronic Army*, available online as of 1 June 2016 from: http://thedesk.matthewkeys.net/2013/12/a-live-conversation-with-the-syrian-electronic-army/

Katerji, O (2013), 'The Syrian Electronic Army Talks About Hacking the 'Guardian' and Their Obama Bomb Hoax', *Vice*, available as of 2 August 2016 from: http://www.vice.com/read/the-syrian-electronic-army-almost-crashed-the-dow-jones

Mumford, A (2013), *Proxy Warfare*, pages 30–45. Polity.

Motherboard (2013), *Is This the Leader of the Syrian Electronic Army?*, available online as of 2 August 2016 from: http://motherboard.vice.com/blog/is-this-19-year-old-the-leader-of-the-syrian-electronic-army

Noman, E, *The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: the Case of the Syrian Electronic Army*, OpenNet Initiative, available as of 2 August 2016 from:

https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army

O'Brien, D (2011), *Syria's Assad Gives Tacit OK to Online Attacks on Press*, Committee to Protect Journalists, available online as of 2 August 2016 from: https://cpj.org/blog/2011/06/syrias-assad-gives-tacit-ok-to-online-attacks-on-p.php and translated from the original, found at: Al-bab.com, Bashar Al-Assad Speech, available as of 1 June 2016 from: http://www.al-bab.com/arab/docs/syria/bashar_assad_speech_110620.htm (no longer available as of 10 August 2016).

Polyanskaya, A, Krivov, A and Lomko, I (2003), *Виртуальный Глаз Big Brother (Virtual Eye of the Big Brother*), available as of 2 August 2016 from: http://www.vestnik.com/issues/2003/0430/win/polyanskaya_krivov_lomko.htm and translated within: Kiyuna, A and ConyersPage, L (2015), *Cyberwarfare Sourcebook*, page 276. Lulu.com.

Roth, A (2016), Vladimir Putin just made it official with actor Steven Seagal's Russian passport, available online as of 2 February 2017 from: https://www.washingtonpost.com/pb/news/worldviews/wp/2016/11/25/vladimir-putin-just-made-it-official-with-actor-steven-seagals-russian-passport/?outputType=accessibility&nid=menu_nav_accessibilityforscreenreader

Robert J B, (1996), *Advanced Battlespace and Cybermaneuver Concepts: Implications for Force XXI*, pages 108-120, available as of 2 August 2016 from: http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/96autumn/bunker.htm

Ravid, B (2012), *Haaretz Exclusive: Organizer of Gaza Flotilla Sought Assistance From Assad's Office*, available as of 15 August 2016 from: http://www.haaretz.com/misc/iphone-article/haaretz-exclusive-organizer-of-gaza-flotilla-sought-assistance-from-assad-s-office-1.411556

Russia Today, (2013), *Anonymous, Syrian Electronic Army Hack Turkish Govt Networks, Leak Emails Incl PM's,* available as of 2 December 2016 from: https://www.rt.com/news/anonymous-turkey-emails-government-252/

Rid, T and Hecker, M (2009), *War 2.0: Irregular Warfare in the Information Age*. Praeger Publishers.

Rid, T and Buchanan, B (2014), 'Attributing Cyber Attacks', *Journal of Strategic Studies*, available as of 17 August 2016 from: https://sipa.columbia.edu/system/files/Cyber_Workshop_Attributing%20cyber%20attacks.pdf

Rozsa, M, (2016), *Donald Trump has spoken to Vladimir Putin as often as he's talked to his intelligence briefers*, Salon, available as of 9 December 2016 from: http://www.salon.com/2016/11/25/donald-trump-has-spoken-to-vladimir-putin-as-often-as-hes-talked-to-his-intelligence-briefers/

Shehabat, A, (2011), *The social media cyber-war: the unfolding events in the Syrian revolution 2011*, available as of 8 December 2016 from: http://www.hca.westernsydney.edu.au/gmjau/archive/v6_2012_2/pdf/ahmad_shehabat_RA_V6-2_2012_GMJAU.pdf

Syrian Ministry of Interior Home Page, available as of 2 August 2016 from: http://syriamoi.gov.sy/new/index.php?req=70

Shapira, H (2013), *Waiting For Jose*. Princeton University Press

Shehaba, A, (2011), *The social media cyber-war: the unfolding events in the Syrian revolution 2011*, available as of 8 December 2016 from: http://www.hca.westernsydney.edu.au/gmjau/archive/v6_2012_2/pdf/ahmad_shehabat_RA_V6-2_2012_GMJAU.pdf

Syrian Freedom (2012), *#Syria's Cyber War,* available as of 2 August 2016 from: https://syrianfreedom.org/syrias-cyber-war

Taber, R (1965), *The War of the Flea: A Study of Guerrilla Warfare Theory and Practise*, 2 August 2002. Brassey's US

WikiLeaks (2012), *Syria Files*, available online as of 2 August 2016 from: https://wikileaks.org/Syria-Files.html

WikiLeaks (2012a), *Syria Files*, available online as of 2 August 2016 from: https://wikileaks.org/syria-files/docs/2101305_.html

WikiLeaks (2012b), *Syria Files*, available online as of 2 August 2016 from: https://wikileaks.org/syria-files/docs/2110828_failure-notice.html

WikiLeaks (2012c), *Syria Files*, available online as of 2 August 2016 from: https://search.wikileaks.org/syria-files/emailid/2101305

WikiLeaks (2012d), *Syria Files*, available online as of 2 August 2016 from: https://wikileaks.org/syria-files/docs/2096858_re-italian-journalists-coming-to-cover-the-visit-of-h-e-the.htm

WikiLeaks (2012e), *Syria Files*, available as of 2 August 2016 from: https://search.wikileaks.org/syria-files/emailid/2351337

WikiLeaks (2012f), *Syria Files*, available as of 15 August 2016 from: https://search.wikileaks.org/syria-files/emailid/2110452

Zambelis, C, (2012), *Information Wars: Assessing the Social Media Battlefield in Syria*, available as of 2 August 2016 from: http://mercury.ethz.ch/serviceengine/Files/ISN/151499/ichaptersection_singledocument/405635ed-f876-447a-a4c6-6decc2fcf27a/en/CTCSentinel-Vol5Iss7_ch6.pdf

Annexes

Annex A

Annex B

Annex C

Annex D