AEI CRITICALTHREATS.ORG
UNDERSTANDING THE CHALLENGE. TRACKING THE THREAT.

AL QAEDA ELECTRONIC:
A Sleeping Dog?

Eric Liu

December 2015

A Report by the Critical Threats Project of
the American Enterprise Institute

Introduction

Cyber warfare is a natural arena for al Qaeda. It allows a small number of covert and dispersed individuals to inflict disproportionate damage on a much stronger adversary.[1] Cyber warriors generally hail from the class of disaffected, educated, relatively-well-off radicals from whom al Qaeda draws its leadership cadres. Al Qaeda should have an advanced cyber-warfare capability to hurt the West and help recruit new followers, but it does not. The only hacking collective claiming affiliation with the group is al Qaeda Electronic (AQE), which was formed only this year and has shown limited and rudimentary capabilities. Al Qaeda does not seem to pose a significant cyber threat to the U.S. or its allies at this time.

Al Qaeda's relative impotence in the cyber realm likely reflects the experiences of its leaders and the group's history. Ayman al Zawahiri, its current leader, and his lieutenants have spent most of the past 25 years operating covertly and trying to evade the prying electronic eyes of Western intelligence agencies. They have seen information technology as a way to communicate securely to a small group of trusted leaders, which is why they still rely heavily on password-protected and tightly monitored closed internet forums and emphasize the virtues of encryption.[2] They have a very defensive mindset when it comes to information technology.[3]

The emergence of the Islamic State of Iraq and al Sham (ISIS) is changing the landscape of al Qaeda-related cyber activities, however. ISIS is much more offensively oriented, and its declaration of an Islamic State shows its desire to operate in the open rather than the shadows. Its use of information technology follows the same pattern. ISIS relies heavily on social media to communicate among its leaders and to its followers, as well as to attract potential recruits. ISIS is creating competition within the jihadi world in cyberspace as well as in the arts of terrorism and atrocity.

Al Qaeda loyalists can evolve dangerous capabilities rapidly in response to this ISIS challenge, should they chose to. Tools for conducting advanced attacks are openly sold on the Dark Web. Cyber capabilities can be easily transferred from criminals to terrorists and among terrorist groups. The relative conservatism and cyber-backwardness of al Qaeda's current leadership should not lull us into complacency. We must still closely follow the individuals and groups claiming to be al Qaeda's vanguard into the cyber war space lest we be surprised one day by an attack that we could have predicted.

Background

Cyber-attackers with limited capabilities generally cannot effectively penetrate and disrupt control software for power grids and other critical infrastructure. Their attacks therefore usually fall into three categories that are more nuisance than major threat, although they can cause significant financial losses to their targets:

- Defacement: The attacker gains access to a website by exploiting misconfigurations and vulnerabilities, and replaces the original content with propaganda or a claim of credit. Particularly motivated attackers may also delete files from the compromised server or upload malware.

- Denial of service (DoS): The attacker renders a website inaccessible to legitimate users by overwhelming it with traffic. A DoS attack can be launched from as few as one computer but its effectiveness increases with the number of machines engaged, as it is harder for cyber-defense systems to handle malicious traffic from multiple clients. Distributed denial-of-service (DDoS) attacks refer specifically to DoS attacks launched from multiple IP addresses.

- Data breach: The attacker breaks into a secured database to access, download, and in some cases publicize the private information contained within. The attacker may infiltrate the target system directly by finding security flaws in the database infrastructure, or indirectly through social-engineering attacks that take advantage of human error (e.g. phishing, baiting).

Early Cyber-Jihadis

The first cyber-jihadi groups emerged in 2006 and focused on vandalizing websites alleged to be anti-Islamic; defacements, which do not rise to the level of a serious threat and are relatively simple from a technical standpoint, remain the most common type of attack perpetrated by such groups. Yet operatives have remained ambitious. An unsuccessful November 11, 2007 campaign tried to use large numbers of al Qaeda supporters simultaneously executing a malicious program to conduct DDoS attacks against a number of Western websites.[4] A post on the Shumukh al Islam jihadi forum in 2011 proposed the creation of a hacking collective focusing on Supervisory Control and Data Acquisition (SCADA) systems of the sort that run critical infrastructure and stock exchanges in the U.S., U.K., and France.[5] A 2012 video released by an al Qaeda operative similarly called for attacks against network-connected infrastructure in the United States.[6] Posters on jihadi websites have, at various points, discussed plans to remotely hijack American unmanned aerial vehicles and drones, power stations and refineries, and communications systems.[7] They do not appear to have led to successful attacks.

False Starts: Claims of an al Qaeda Electronic Group in 2013-2014

References to a cyber-army directly affiliated with al Qaeda appear in sites frequented by hackers and on social media beginning in 2013, but none of these groups are likely related to the present-day al

Qaeda Electronic or any recognized al Qaeda affiliates. They may not have existed at all, in fact, except as names.

Al Qaeda Electronic in Egypt

SITE Intelligence Group first reported a rash of attacks by "ABO aBYDa Al MaSReY" (Abu Obeida al Masri) on December 31, 2012, and a search on Zone-H, a website on which hackers boast about their exploits, brings up hundreds of attacks under a similar alias.[8] Al Masri's real identity and affiliation are unclear. His name is likely a pseudonym, perhaps in honor of the Egyptian-born al Qaeda operative linked to the 2005 London bombings (al Masri means "the Egyptian").[9] He has claimed via his defacement pages to be affiliated with "al Qaeda Electronic in Egypt" and later, "the Islamic Electronic Army;" but there is no discernible connection between al Masri and any hacking collective.[10]

Al Masri's activity also predates the first mention of the present-day AQE, in 2015, but the two groups could still be associated. Technical and rhetorical commonalities link al Masri with Yahya al Nemr, the current leader of AQE. Both hackers' defacement pages prominently display the flag of al Qaeda in the Arabian Peninsula (AQAP), employ rhetoric about Palestinian freedom, and rely on similar mechanisms of attack.[11] Al Nemr's Zone-H account (active since October 2013) began to report attacks shortly after activity on al Masri's (active until September 2013) ceased, moreover, and al Masri dedicated his first attacks to Abu Dujana al Khorasani – an al Qaeda operative known for a suicide attack against Forward Operating Base Chapman in Khost, Afghanistan – linking both al Masri and al Nemr, who has likely lived in Kandahar, to Afghanistan.[12]

There is no definitive evidence linking al Masri and al Nemr, however, and there are alternate explanations for the similarities: there is nothing idiosyncratic about the rhetoric or circumstances of the two cyber-jihadis, and al Nemr may have come across al Masri's work by chance and sought to mimic it. Al Masri and al Nemr could be the same person, but it is at least equally plausible that al Masri used both the Islamic Electronic Army and al Qaeda names simply to bolster his legitimacy and was not connected to al Nemr, al Qaeda, or any other organization.

AQE in Operation Black Summer

The al Qaeda Electronic brand emerged elsewhere in February 2013, while al Masri was still active, when a group under that name announced an anti-American cyber operation codenamed Black Summer in partnership with the Tunisian Cyber Army (TCA). The effort penetrated a number of prominent websites, several of which belonged to U.S. government agencies and multinational corporations, between February and May.[13] The use of the AQE brand was probably meant purely to enhance the reputation of the TCA, however, since it does not appear that there was any independent al Qaeda-affiliated hacking group involved in the attacks.

The history and involvement of the TCA is well documented, particularly as it was the public face of the operation. Its leader and only identified member to date, Fahmi Ben Khalifa, demonstrated considerable expertise and sophistication, gaining unauthorized access to databases.[14] He personally executed a number of notable hacks prior to Black Summer, including against domains belonging to the French Ministry of Defense and NASA.[15]

The existence of a separate al Qaeda Electronic group in this operation is much less certain, as it did not release a statement officially declaring its participation. Mentions of AQE are always in the context of its partnership with the TCA.[16] The entities targeted in Black Summer, as well as the techniques and tactics employed, were vastly more sophisticated than those associated with al Masri, al Nemr, or any other known group with potential links to al Qaeda as well.

Moreover, the operation was intended to formally begin on May 31, 2013 and continue throughout the summer, yet reports of new activity related to the campaign – and further mentions of AQE – ceased after May 2, five days before Khalifa's arrest by Tunisian authorities.[17] The subsequent radio silence suggests that the attacks leading up to that point had been coordinated by Khalifa, and calls into question the existence of AQE.[18] Khalifa's sole declared motivation to "prove to all those who think that they are a great administrator [sic] that they need more security" also does not align with al Qaeda's political goals and rhetoric.[19] His decision to work in the white-hat computer-security industry upon his release from prison further calls into doubt the authenticity of a collaboration with anti-Western terrorist groups.[20]

These observations support the hypothesis that the TCA exaggerated its attacks and collaborations in order to "leverage fear…while developing credibility and notoriety," as posited by the National Cybersecurity and Communications Integration Center.[21] It is probable that the entity described as al Qaeda Electronic in the Black Summer announcements did not exist at all.

Al Qaeda Electronic Emerges

Formation

Al Qaeda Electronic announced its formation as a new branch of al Qaeda focused on cyber-warfare in a brief video on January 20, 2015.[22] The unnamed narrator identified Yahya al Nemr as the leader of the group, though most of the video was spent justifying hacking as a valid form of jihad. The organization reposted the video in subsequent days predominantly on jihadi forums to recruit members and generally increase awareness of the brand. This initial publicity campaign was moderately successful in terms of reach—one video-hosting site reported over 10,000 views—but the reaction was muted and some commentators questioned the group's legitimacy.[23]

A number of media outlets that covered the announcement attributed it to al Qaeda.[24] However, there is no evidence directly confirming the involvement of al Qaeda general command, and the claim appears to be an unsubstantiated extrapolation from AQE's self-declared name.

Connection to al Qaeda

The strongest indication of a relationship comes from a trip apparently taken by AQE's leader, Yahya al Nemr, to al Mukalla, Yemen, in late March and early April 2015, and his potential involvement in a major prison break there during that visit. These events, if confirmed, would make it probable that al Qaeda Electronic, which al Nemr leads, has some connection to AQAP, though the strength of the association cannot be determined without further evidence.

The storming of al Mukalla's central prison on April 2, 2015, during which at least two senior officials affiliated with al Qaeda in the Arabian Peninsula escaped, was attributed to AQAP militants.[25] The fact that al Nemr travelled to the region a week in advance and claims to have participated in the attack itself therefore links him to AQAP. The facts of this story are sourced from a series of posts by al Nemr on his Facebook profile. He checked in via a geotagged post to Hadramawt governorate, of which al Mukalla is the capital, on March 26; posted about the liberation of prisoners and the fight against the "apostate" police on the evening of April 2; and checked back in to Kandahar province, his purported residence, on April 11.[26] It is possible that al Nemr spoofed the locations tagged in the posts, but the timestamps are immutable and the number of interactions from his Facebook friends suggest that they believed he was in Yemen. It is a reasonable supposition, therefore, that al Nemr was affiliated with AQAP at the time of the event and remains so today.

Leadership

Yahya al Nemr (Emir)

Al Nemr is the face of al Qaeda Electronic, whereas AQE's four other members do not have individual public presences. He often publishes details about AQE and its members directly instead of through al Maarek, the group's official media arm, and is the only source of information about details such as the group's physical location. Al Nemr has moreover been accessible to his followers and potential recruits since before the formation of AQE and remains so to this day. He has created and advertised at least three personal Facebook profiles, two of which remain active and one that is largely public; two email addresses; and a Skype account.[27]

Information drawn from these accounts suggests that al Nemr was born in Tikrit, Iraq; lived in al Arish, Egypt for some period of time; relocated to Kandahar, Afghanistan; and finally moved back to al Arish, where he currently resides.[28] These locations line up with the geographical foci of his activities: he frequently included pictures of Saddam Hussein in his posts on jihadi forums and his defacement pages; AQE attacked an Egyptian news outlet in May 2015; and he has posted on several occasions about the Islamic Emirate of Afghanistan and Mullah Mohammed Omar Mujahid, the former leader of the Taliban and commander of the faithful during the time of the Islamic Emirate, including prior to the confirmation of Mullah Omar's death in July 2015.[29]

These locations and iconographies are problematic in another sense, however. Iraqi Ba'athists venerated Saddam, and many have become important figures in ISIS (and Tikrit was Saddam's home town). It is rather more unusual to find an al Qaeda loyalist from Iraq openly supporting Saddam, however. Al Arish is the main city in the Sinai Peninsula, where ISIS is the predominant jihadi group. It is, again, odd for an anti-ISIS al Qaeda hacker to locate himself there. Kandahar is a particularly unlikely location for a hacker of any orientation because of the lack of reliable electricity and internet access. There is no obvious reason for al Nemr to have invented these locations for himself, on the other hand, so these oddities may just be oddities. They remain worth noting nevertheless and must reduce our confidence in al Nemr's posts about himself.

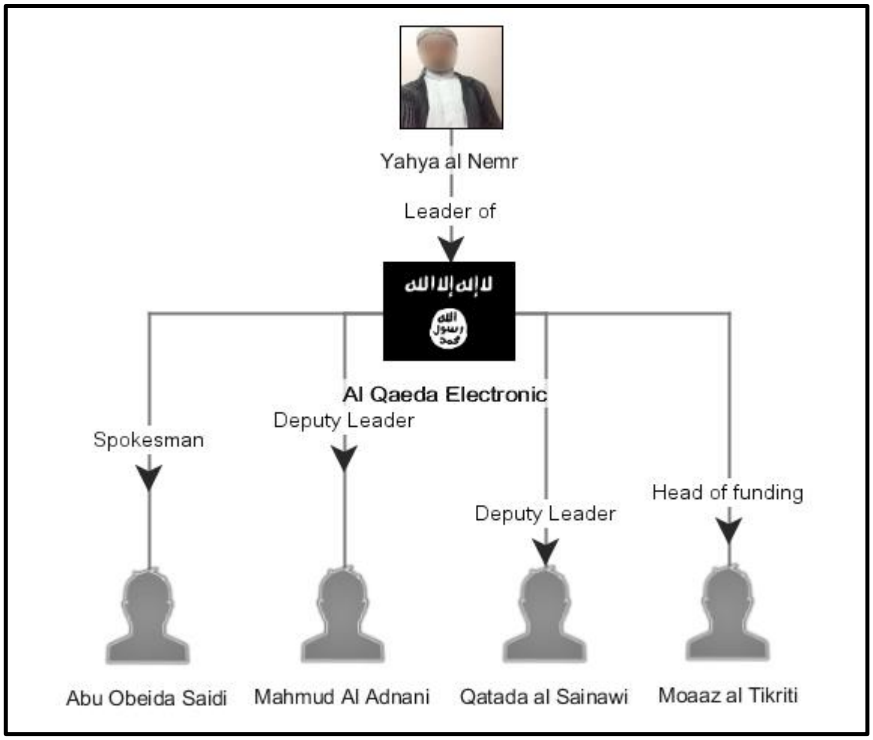

Figure 1: The known members and leadership structure of al Qaeda Electronic
Source: Author and AEI's Critical Threats Project

Mahmud al Adnani (Deputy Emir)

On January 27, 2015, al Nemr posted to his Facebook account a purported screenshot of a U.S. Central Command (CENTCOM) announcement offering a reward for information leading to the capture of "Yahya Al nemr a member of al Qaeda and leader of al Qaeda Electronic" and "his deputy Mahmoud Al adnani."[30] Al Nemr almost certainly forged the image, as the text is riddled with errors and the official U.S. CENTCOM Facebook page shows no record of it. The post can thus be viewed as confirmation from al Nemr himself of his relationship to al Adnani. Al Adnani's public presence is limited to his sparse Facebook profile, which lists his birthplace as al Arish.[31]

July leadership announcement: Qatada al Sainawi (Deputy Emir), Moaaz al Tikriti (Funding Officer), Abu Obeida al Saidi (Spokesman)

Al Maarek Media published an official statement on July 6, 2015, naming Qatada al Sainawi as "deputy emir" and describing Moaaz al Tikriti as being "responsible for funding."[32] The announcement briefly introduced the two as AQE's former spokesman and a former fighter for al

Qaeda in Iraq, respectively.[33] Al Sainawi has not released any public statements to date, in spite of his former position.

Al Maarek did not mention al Adnani in the announcement, but al Nemr linked to his Facebook profile and invited readers to follow the "deputy emir of al Qaeda Electronic" on July 13, a week after the al Maarek statement.[34] Al Adnani thus appears to have remained in his position as deputy emir, alongside the new appointee.

Al Nemr also made the announcement of al Sainawi's replacement separately, encouraging supporters to follow the group's new spokesman, Abu Obeida al Saidi, in a Facebook post on July 14.[35] Al Saidi also maintains a Facebook account, but he too has yet to publish a statement.[36]

Activities

Targets and techniques

Most of al Qaeda Electronic's cyber-attacks consist of website defacements against relatively low-value targets. The group has launched occasional denial-of-service attacks as well, though there is no external confirmation of the success of these efforts since the targets are relatively obscure. AQE has yet to attempt an attack against a high-traffic or otherwise notable website, such as one belonging to a government agency or multinational corporation, nor has it released data from secured databases, which have become common targets for other hacking teams.

The group has been intermittently active since its formation in January 2015. It tends to conduct a series of attacks on consecutive days, often hitting multiple sites on the same day, interspersed with weeks of inactivity. There are some signs of an attempt to time attacks to symbolically important periods – after a two-month lull, the group significantly increased its activity on June 12, 2015 and consistently defaced websites through July 16, overlapping Ramadan – but it has shown opportunistic streaks as well, twice taking down forums after they were accused of supporting the Islamic State by the hacking collective Anonymous.

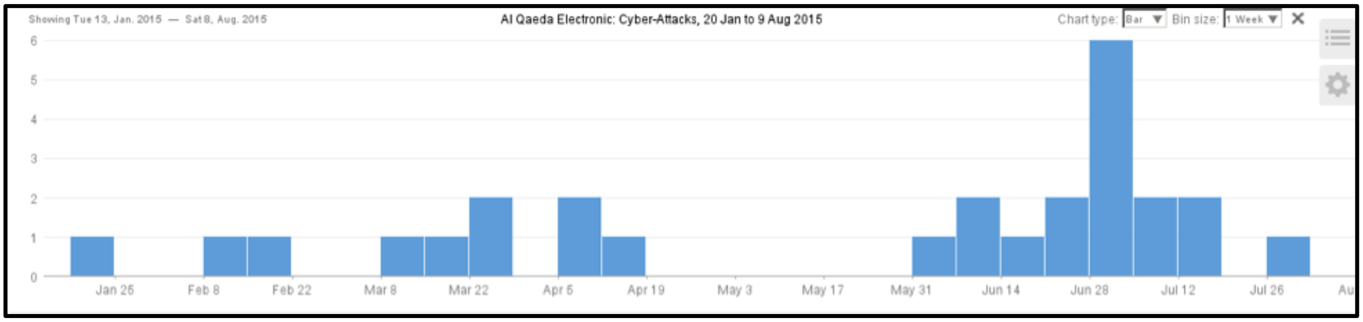

Figure 2: A histogram of attacks conducted by al Qaeda Electronic since its inception, January 20, 2015, to August 9, 2015
Source: Author and AEI's Critical Threats Project

Publicity

Al Qaeda Electronic routes all of its official announcements, typically in both Arabic and imperfect English, through its media outlet, al Maarek. The bulk of al Maarek's publications report on AQE's cyber-attacks, though the agency has occasionally posted on general-interest topics relating to al Qaeda, such as the death of AQAP head and al Qaeda operations manager Nasser al Wahayshi.[37]

AQE typically posts its hacks to sites such as Zone-H.org, Zone-HC.org, and Mirror-Zone.org, which permanently record and mirror defaced web pages so that they can be viewed indefinitely, even after the targeted site itself removes the defacement. Al Maarek then follows by announcing the attacks on Facebook and Twitter as well as various jihadi forums.[38] The outlet was more elaborate in publicizing AQE's first few successes as well as its rare denial-of-service campaigns. It released videos to commemorate the group's first attack, a DoS campaign against a Panama-based financial services company on January 23, 2015, and subsequent penetrations of USArmy.com (unaffiliated with the United States Army) on February 8 and al Faraeen, an Egyptian media outlet, on May 31.[39] The last production was particularly unusual in its specificity, accusing the station manager, Tawfiq Okasha, of being associated with Mossad and working against Islam to "[defend] the Zionist Jews."

Al Maarek has omitted this level of detail from its more recent statements, opting instead to release uniformly structured and briefly annotated lists of targeted websites. This shift likely reflects the increasing blandness of AQE's attacks – even its supporters would find it difficult to link the group's recent, scattershot defacements to its anti-Western and pro-Palestinian rhetoric – but could also arise from a belief among AQE and al Maarek operatives that they are sufficiently well-established in the jihadi community to make further high-production-value advertisements unnecessary.

Defacement characteristics

AQE's typical defacement attack involves replacing the content of the targeted website with a single identical page proclaiming that the site has been hacked. The limited text, in English and Arabic, expresses pro-Palestinian and anti-Western sentiments, and is adapted from a quote by Osama bin Laden in a 2013 issue of *Inspire*, an online magazine published by AQAP to reach English-speaking Muslims.[40] The defacement page additionally displays a series of images, including AQAP's flag, the Black Standard, and a picture of Osama bin Laden and Ayman al Zawahiri. Credit for the hack is clearly attributed to al Qaeda Electronic, and an embedded Twitter feed at the bottom points to al Maarek's Twitter account, though individual members of the group are not identified.

Two signature technical attributes are that the standard cursor is replaced with a crosshair, and right clicking is disabled. The HTML source code further reveals that all media assets are uploaded to an external file hosting service (http://arab(.)sh), instead of the server of the targeted website; and that the HTML file was generated by Microsoft Word 2003. These idiosyncrasies are also present in the defacement page used by al Nemr in his individually credited attacks. The similarities between the two are beyond coincidental and imply that al Nemr has had a strong technical role in AQE's operations to date.

Capabilities

Al Nemr conducted over 300 defacements prior to the announcement of AQE's launch. These attacks, which primarily took place over an eight-month period from October 2013 to May 2014, closely mirror those carried out by AQE in terms of targets, techniques, and style, providing additional evidence that al Nemr is the lynchpin of al Qaeda Electronic.[41]

Recruitment

AQE is currently a relatively small organization with five claimed members, and while numbers are comparatively less important for an electronic-focused group due to the asymmetric nature of cyber-warfare, there are still compelling reasons for the group to expand. More hackers would certainly bolster the nascent entity's legitimacy and enhance its ability to conduct higher-profile and more sophisticated attacks. It is therefore highly relevant that al Nemr has led at least one hacking collective before AQE, since that potentially provides him with a valuable network of associates to tap.

He is most clearly linked to the "Forces Iraq Electronic" (FIE), a hacking collective that defaced at least 94 websites over a four-month period from January 6 to April 21, 2014. The FIE promoted its activities primarily on its Facebook page, claiming to hack websites that were American or Jewish, or hosted anti-Islamic content, in defense of Iraqi interests and Islam.[42] Its publicly claimed leadership consisted of al Nemr as commander, "SWAT Ghost Baghdad" as the commander of special operations, Abu al Mashakl as the attorney general, "Lion Diyala" as the commander of intelligence forces, and "Prince Hacker" as the spokesman.[43]

A second statement on March 24 declared the expulsion of SWAT Ghost Baghdad and al Qaisi from FIE, without naming their successors or providing an explanation. Neither alias appeared on the group's defacement pages thereafter, though three new ones – Sakar al Karada, Ali al Kaabi, and "!-_*YaSSeR*_-! – did begin to receive credit.[44] The emails and Facebook profiles provided for these new members differed from those of SWAT Ghost Baghdad and al Qaisi, so the March expulsion was unlikely to be a hoax – it is uncertain what benefit would accrue to the FIE in that case anyway – leaving the possibility of a genuine disagreement within the organization.

A second group identifying itself as "Team AlHackers AlMujahidin" conducted at least two defacements against privately owned websites.[45] The list of members credited was the same in both attacks: in order, al Nemr (under his common pseudonym Yahya al Saddami), al Mashakl, 'Alwaawi al Malik, and "Ahtrafi."[46] The latter two names do not appear on the FIE's defacement pages and likely refer to distinct individuals.

In sum, Al Nemr has established and maintained relationships with at least seven operatives, each of whom likely possesses at least a basic set of technical skills, through these groups. None of these names has appeared in connection with AQE thus far, but it is certainly possible that the same individuals are working under new aliases, or that al Nemr may look to recruit them in the future.

Technical competencies

The Facebook page of the Forces Iraq Electronic made its first public post on January 4, 2014, and advertised its official forum, located at Sec-Iraq.Koom.ma, in an advertisement published three days later. Al Nemr and several other FIE members maintained readily identifiable accounts on the forum, though al Nemr's saw a particularly high amount of activity, with 182 contributions from the creation of the account in May 2013 to the time of his last post in April 2014.[47] These messages color in our understanding of al Nemr's and FIE's techniques and skill level.

Only one of al Nemr's replies came in a thread providing a tutorial of exploitation techniques; the rest were in response to links and guides to particular software programs, an indication that he was more interested in amassing a collection of ready-to-use tools than building up his expertise. Specifically, al Nemr posted in several discussions on the use of remote access Trojans (RATs) that grant the attacker full control over the targeted computer, including Bifrost, njRAT, and XtremeRAT, as well as programs to disguise RATs within seemingly innocuous files; he also started a thread on this subject, the only technical one attributed to his account.[48] Al Nemr further expressed interest in programs capable of conducting denial-of-service attacks, scanning websites and networks for vulnerabilities, obfuscating IP addresses, and enabling port forwarding.[49]

It is probable that al Nemr used several of these tools, especially the vulnerability scanners, to carry out his attacks. In particular, he likely combined these software programs with scripts that automatically report successful penetrations to mirroring databases, which would explain his behavior of mass defacements and tendency to report the same URL with slightly different defacement pages to multiple mirroring sites. The single-computer DoS programs discussed on Sec-Iraq are moreover likely to have been sufficient for the limited denial-of-service attacks that he has managed so far.

Al Nemr was also an active participant on the message boards of Aljyyosh.com, a defacement-mirroring site. The majority of his 103 posts there repeated claims of cyber-attacks by the FIE, but he did post links to two versions of a "Forces Iraq Electronic browser," a very basic Internet browser that does not appear to have any special functionality and does not seem to cloak malicious code.[50] However, it does demonstrate a basic competency on the part of al Nemr and his colleagues to code, package, and distribute a product.

Notably, neither al Nemr individually nor any of his affiliated organizations have claimed to have stolen credentials, captured screen recordings of targeted computers, or succeeded in any other attack that would suggest the deployment of remote access Trojans. The most plausible explanation is a lack of skill; al Nemr and AQE are unlikely to be uninterested in accessing sensitive systems but rather lack the know-how to successfully place the malware on their targets. Threads on Sec-Iraq forum indeed did not discuss strategies to deploy software onto target systems, focusing only on the mechanics of creating the malware and establishing access to a remote computer. Thus, RATs and other social-engineering attacks that trick human users into giving up credentials and other sensitive information, such as phishing, are probably out of reach for AQE for now, requiring a significantly higher level of technical understanding and skill than has been demonstrated so far.

Conclusion

Al Qaeda Electronic's attacks to date have shown little finesse and the group has almost certainly relied heavily on automated vulnerability scanners to find points of penetration. It is unlikely that its program of defacements is merely a distraction for a more menacing operation, such as the covert formation of a botnet, since there is no indication that AQE's members have the requisite technical skills and the group has not promised to target specific institutional or other large, high-value targets.[51] Rather, AQE has not been able to move beyond opportunistic and low-effort defacements in the eleven months since its formation. Its attacks have not increased in sophistication and its public statements do not indicate an imminent ramping-up of aggressiveness either.

However, al Nemr and AQE's members are aware of, and on certain occasions have executed, more advanced tactics, and it remains plausible that AQE could move onto targets of greater importance and deploy more powerful software. The group has expended a considerable amount of effort on organizational formalities, including creating a leadership hierarchy and establishing a separate media outlet. AQE's social media arm, al Maarek, moreover, has noticeably avoided exaggeration in its statements, in contrast to the Forces Iraq Electronic's tendency to falsely claim attacks against high-value targets.[52] All of this indicates that AQE's members are serious about their work and hope to establish a legitimate and durable presence in the online jihadi community for themselves. Al Nemr's experiences in leading similar hacking collectives, network of associates, and record of cyber-attacks tracing back to at least October 2013 bolster the potential for escalation. Finally, AQE's connection to AQAP opens the possibility that the latter could provide valuable assistance with recruiting; in the digital realm, the addition of even a single experienced member could dramatically raise the group's overall capabilities.

Al Qaeda Electronic is a weak first foray into cyber-offensive operations for al Qaeda, if the two are indeed connected. AQE does not pose a threat currently to its predominantly Western targets, lacking the personnel, technical abilities, and history of successes that would be necessary to rank it on par with better-known cyber actors like the Syrian Electronic Army, let alone state-operated units. Yet it cannot be immediately written off, for two reasons. First, there is still a real potential for AQE to evolve into a more dangerous entity, considering the history and connections of its members. Second, and more significantly, AQE's emergence underscores the low barrier to entry in the cyber-sphere: five untrained fighters pose a negligible threat in the physical realm but can legitimately target disproportionately large enemies online. This group may never develop into the electronic standard-barrier of al Qaeda, but its failure to do so would not entail the dissipation of the underlying cyber-threat. Other jihadi hackers will surely try again, and, especially if al Qaeda leadership emerges with a stronger electronic focus, we may well see the brand reincarnated in the future as a truly formidable force.

Notes

[1] Andrew Phillips, “The Asymmetric Nature of Cyber Warfare,” US Naval Institute News, October 14, 2012, http://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare; William J. Lynn III, “Defending a New Domain: The Pentagon’s Cyberstrategy,” *Foreign Affairs* 89, no. 5 (September/October 2010), https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

[2] “How Al-Qaeda Uses Encryption Post-Snowden (Part 2) – New Analysis in Collaboration with ReversingLabs,” Recorded Future, August 1, 2014, https://www.recordedfuture.com/al-qaeda-encryption-technology-part-2/.

[3] What limited effort al Qaeda has expended on offensive operations has centered on propaganda dissemination instead of cyber warfare proper. For instance, a cover story published in the al Qaeda-linked *Inspire* magazine discussed the importance of combating Western ideology through “powerful media production[s];” and Osama bin Laden wrote that the “wide-scale spread of Jihadist ideology, especially on the Internet, and the tremendous number of young people who frequent the Jihadist websites” was a “major achievement for Jihad.” See: Samir Khan, “The Media Conflict,” *Inspire* 7 (September 2011): 9-10, https://publicintelligence.net/inspire-al-qaeda-in-the-arabian-peninsula-magazine-issue-7-september-2011/; Osama bin Laden to Shaykh Mahmud (‘Atiyya), translated by the Combating Terrorism Center, May 2010, in CTC Letters from Abbottabad, no. SOCOM-2012-0000019, Combating Terrorism Center at West Point, https://www.ctc.usma.edu/posts/letters-from-abbottabad-bin-ladin-sidelined, 2.

[4] Andrew Campbell, “‘Electronic Jihad’ November 11 Attack Fails to Materialize,” Daily Tech, November 13, 2007, http://www.dailytech.com/Electronic+Jihad+November+11+Attack+Fails+to+Materialize/article9646.htm.

[5] “Jihadist Organizes Center for E-Jihad,” SITE Intelligence Group, June 13, 2011, https://ent.siteintelgroup.com/Social-Network-Jihad/site-intel-group-6-13-11-jfm-e-jihad-center.html.

[6] Jack Cloherty, “Virtual Terrorism: Al Qaeda Video Calls for ‘Electronic Jihad,’” *ABC News*, May 22, 2012, http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875.

[7] Steven Stalinsky and R. Sosnow, “From Al-Qaeda To The Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad,” *Middle East Media Research Institute* (December 2014), hanttp://cjlab.memri.org/wp-content/uploads/2014/12/cyber-jihad-2.pdf, 12–16.

[8] Arabic for Abu Obeida al Masri: ابـّو عـبـيـدة إلـمـَصـري; “Jihadist Hacks Websites to Commemorate CIA Base Attack in Khost,” SITE Intelligence Group, December 31, 2012, https://ent.siteintelgroup.com/Jihadist-News/jihadist-hacks-websites-to-commemorate-cia-base-attack-in-khost.html; link to the profile of “abyda al masrey” on Zone-H.

[9] Craig Whitlock and Karen De Young, “Senior Al-Qaeda Commander Believed to be Dead,” *Washington Post*, April 10, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/04/09/AR2008040901793.html?hpid=moreheadlines.

[10] Arabic: تنظيم القاعدة الالكتروني في ارض الكنانة (al Qaeda Electronic in Egypt) and جيش الاسلام الالكتروني (Jaysh al Islam al Elektroni).

[11] Both hackers appear to focus on opportunistic defacement attacks that exploit known vulnerabilities, instead of targeted attacks against particular websites or systems of interest. Both also seem to follow a similar procedure of defacing multiple sites in the span of a few days, then reporting them to Zone-H and other mirroring websites. Additionally, the defacement pages of al Masri and al Nemr both borrowed source code from http://star28(.)com, which is a directory of online Arabic resources, and Microsoft Word’s HTML conversion feature.

[12] Link to a mirror of the first attack reported by al Nemr on Aljyyosh.org, another online defacement archive.

[13] “Electronic al-Qaeda Army claims to have hacked US government websites,” RT, March 11, 2013, http://www.rt.com/usa/hacked-us-government-websites-112/; Eduard Kovacs, “US Department of State, Pentagon Websites Hacked by Tunisian Cyber Army,” Softpedia, March 11, 2013, http://news.softpedia.com/news/US-Department-of-State-Pentagon-Websites-Hacked-by-Tunisian-Cyber-Army-336016.shtml; Eduard Kovacs, “OpBlackSummer: US Government Sites CBP.gov and OPM.gov Reportedly Hacked,” Softpedia, March 13, 2013, http://news.softpedia.com/news/OpBlackSummer-US-Government-Sites-CPB-gov-and-OPM-gov-Reportedly-Hacked-336836.shtml; Sabari Selvan, “#opBlackSummer: Two US Petroleum companies websites breached by AQEA & TCA,” E Hacking News, March 14, 2013, http://www.ehackingnews.com/2013/03/opblacksummer-two-us-petroleum-websites.html.

[14] Khalifa frequently used the aliases “XTnR3v0lt” and “fahmi_TCA” online. He likely possessed real and significant skills, in particular relating to the exploitation of XSS and SQL injection vulnerabilities, that went beyond defacements.

[15] Sabari Selvan, “French Ministry of Defense hacked and database leaked by XTnR3voLT,” E Hacking News, January 15, 2013, http://www.ehackingnews.com/2013/01/france-ministry-of-defense-hacked.html; Waqas Amir, “#opleak: French Ministry of Defense Breached, Database & Login Info leaked by @XTnR3voLT,” HackRead, January 15, 2013, https://www.hackread.com/opleak-french-ministery-of-defense-breached-database-login-info-leaked-by-xtnr3v0lt/; Sabari Selvan, “#opleak29: NASA database leaked by xl3gion hackers,” E Hacking News, January 7, 2013, http://www.ehackingnews.com/2013/01/opleak29-nasa-database-leaked-by.html.

[16] All statements were released through the Tunisian Cyber Army’s online accounts, as this incarnation of AQE apparently did not have its own presence. The strongest indication of AQE’s existence is a video allegedly issued by the group in which the narrator, Ahmad bin Laden, declares the goals of Operation Black Summer. However, bin Laden’s name does not appear elsewhere, and the video itself seems to have been publicized only on the TCA’s Facebook page. It is plausible that the video actually originated from the TCA itself and not AQE, since the rhetoric closely matched other messaging from the TCA in promising severe attacks on American electronic infrastructure, and we do not see any individuals in the video. Information about the video was sourced from SITE.

[17] Kohlmann, Twitter post.

[18] Selvan, “Petroleum companies websites breached.”

[19] Lee J, “Interview with @XTnR3v0LT from xl3gion,” Cyber War News, November 8, 2012, http://www.cyberwarnews.info/2012/11/08/interview-with-xtnr3v0lt-from-xl3gi0n/.

[20] The authenticity of Khalifa’s interest in exposing vulnerabilities in software for the sake of stronger security, as opposed to any malicious ends, is bolstered by his record of work since his release from prison (he was apparently sentenced to a year in prison beginning in November 2013 [Facebook]). He has received multiple acknowledgements from large technology companies, including ESET, a Slovakian IT security company (Beast: Twitter, XSS: Twitter); Avira, a German security company (XSS: Twitter); Sony, a Japanese electronics conglomerate (Hall of Thanks entry); Lavasoft, a German anti-malware company (Facebook); and Oracle, an American technology company (CPU advisories from Apr. 2014, Oct. 2014, and Jan. 2015. He has also publicized a number of exploits seemingly for purely informational purposes (demonstrations [Facebook] of live exploits at a Tunisian white-hat security conference, Facebook XSS attack [Twitter], Central Bank of Belize XSS attack [Twitter], Central Bank of Azerbaijan XSS attack [Twitter]).

[21] US Department of Homeland Security, National Cybersecurity and Communications Integration Center, *Tunisia Cyber Army*, March 27, 2013, 3, http://dropbox.curry.com/ShowNotesArchive/2013/04/NA-503-2013-04-11/Assets/Cyber%20War$/AQECA.pdf.

[22] Original Arabic username of the account: الالكترونيه الجهاد قاعدة. Link to the video on Archive.org.

[23] Link to the video on Archive.org reporting over 10,000 views. Two posters on al Aren, a jihadi forum, pointed to grammatical errors in the narrator’s statement and raised doubts about the group’s ties to al Qaeda: link to thread.

[24] Mustafa Ahmad, “Al Qaeda announces al Qaeda Electronic,” *Khabar*, January 21, 2015, http://www.alkhabar.ma/الالكتروني-القاعدة-تنظيم-قيام-يعلن-القاعدة-تنظيم_a69741.html; Dimitry Shvartsman et al., “Al Qaeda’s Electronic Jihad,” *SenseCy*, February 2, 2015, http://blog.sensecy.com/2015/02/02/al-qaedas-electronic-jihad/.

[25] Alexis Knutsen, “2015 Yemen Crisis Situation Report: April 3,” AEI’s Critical Threats Project, April 3, 2015, http://www.criticalthreats.org/yemen/yemen-crisis-situation-reports-april-3-2015; Louisa Loveluck and Magdy Samaan, “Al-Qaeda frees prisoners in Yemen jail break,” *Telegraph*, April 2, 2015, http://www.telegraph.co.uk/news/worldnews/middleeast/yemen/11512811/Al-Qaeda-frees-prisoners-in-Yemen-jail-break.html.

[26] Links to posts on al Nemr’s Facebook profile: first check-in to Hadramawt on March 26, second check-in on March 27, post about the prison break on April 2, check-in to Kandahar on April 11.

[27] Arabic: النمر يحيى (Yahya al Nemr). Facebook accounts: mujahed.yahyanemr, almujahed.yahyanemr, almujahed.yahyabanna (inaccessible). Yahoo emails: yahya.saddami@yahoo.com, yahya.banna@yahoo.com.

Skype handle: yahya.saddami. This data was collected from his defacement pages as mirrored on Zone-H; see representative samples here and here.

[28] These details are self-reported on al Nemr's active Facebook accounts. The accounts are likely to be authentically his given the high volume of posts about al Qaeda Electronic and cross-interactions between these accounts and al Maarek's Facebook page, which include al Maarek sharing one of al Nemr's posts and al Nemr posting a link to al Maarek's page.

[29] Link to a thread started by al Nemr on Sec-Iraq forum with a number of pictures of Hussein.

[30] Link to the image on Facebook. Al Adnani's name in the original Arabic: لمحمود العدناني.

[31] Link to al Adnani's profile on Facebook.

[32] "'Al-Qaeda Electronic' appoints alleged AQI fighter to oversee funding efforts," SITE Intelligence Group, July 6, 2015, https://ent.siteintelgroup.com/Statements/al-qaeda-electronic-appoints-alleged-aqi-fighter-to-oversee-funding-efforts.html.

[33] "'Al-Qaeda Electronic' appoints alleged AQI fighter," SITE Intelligence Group.

[34] Link to al Nemr's post on Facebook.

[35] Original Arabic: ابو عبيدة الصعيدى (Abu Obeida al Saidi). Link to al Nemr's post on Facebook.

[36] Link to al Saidi's profile on Facebook.

[37] Link to a eulogy for Wuhaysi [Twitter] from al Maarek.

[38] Links to al Maarek Media's Facebook page and Twitter feed.

[39] Links to videos by al Maarek on the Coyalta hack [YouTube], the USArmy.com hack [Archive.org], and the al Faraeen hack [Archive.org].

[40] Examples include an assertion of Palestinian statehood on this typical defacement page [Zone-H] and a promise to attack the economies of America and its allies in a forum post [NationalKuwait.com]; Shaykh Abu Mus'ab al Awlaki, "Why Did I Choose al Qaeda? Today's Reasons: The Hadeeth of Al-Malahem," *Inspire* 10 (March 2013): 34, https://azelin.files.wordpress.com/2013/03/inspire-magazine-issue-10.pdf; Katherine Zimmerman, "Expanding the Campaign of Violence: Al Qaeda in the Arabian Peninsula's English-Language Magazine," American Enteprise Institute, July 13, 2010, http://www.criticalthreats.org/yemen/expanding-campaign-violence-al-qaeda-arabian-peninsulas-english-language-magazine-july-13-2010.

[41] Al Nemr's aliases on mirroring sites include "Yahya AlNemr," "Yahya AlSaddami," and "Yahya Tiger." He or one of his associates are likely to be reporting attacks by AQE to these same sites, under the aliases "Al-Qaeda Electronic" and "AlQaeda Electronic."

[42] Arabic: القوات العراقيه الالكترونيه (Forces Iraq Electronic). Link to the group's main page, and the About tab where they describe their mission, on Facebook. Most of their attacks were reported to Zone-H.org, under one of al Nemr's aliases, "Yahya AlSaddami."

[43] Arabic: ابو المشاكل (Abu al Mashakl), سوات شبح بغداد (SWAT Ghost Baghdad), بسام القيسي (Bassam al Qayassi), اسد ديالي ("Lion Diyala"), العراق هكر برنس ("Prince Hacker"). Link to the first leadership announcement on Facebook. Link to al Mashakl's profile on Facebook. "Lion Diyala" is an alias for Bassam al Qaisi. This leadership announcement accounted for all of the names that had appeared at least once on the FIE's defacement pages, except "~!SpEcTeR-HMoODY-!~." However, that name is likely an alias of Prince Hacker, since SpEcTer's byline in the Sec-Iraq forum describes him as the group's spokesman as well, and the timelines of the two pseudonyms do not overlap. Link to SpEcTeR's profile on Sec-Iraq forum. His byline in the original Arabic reads: المتحدث الرسمي بأسم القوات العراقيه الالكترونيه.

[44] Arabic: صكار الكراده (Sakar al Karada), علي الكعبي (Ali al Kaabi), and ياسر دوله وعلم ("!-*YaSSeR*-!").

[45] Arabic: منظمة الهكرز المجاهدين. Link to the group's profile on Zone-H, which is attached to one of their two confirmed attacks.

[46] Original Arabic: علاوي الملك (Alwaawi al Malik) and احترافي ("Ahtrafi").

[47] Links to the accounts of al Nemr, SWAT Ghost Baghdad, and al Mashakl on Sec-Iraq forum. ~!SpEcTeR-HMoODY-!~ also maintained an account on the forum, as linked above.

[48] Links to relevant threads on Sec-Iraq forum, by topic: Bifrost (Thread 1, Thread 2, Thread 3), njRAT (Thread 1, Thread 2, Thread 3, Thread 4, Thread 5, Thread 6), XtremeRAT (Thread 1, Thread 2, Thread 3), RAT injectors (Thread 1, Thread 2, Thread 3, Thread 4, Thread 5). Link to thread started by al Nemr on Sec-Iraq forum.

[49] Links to relevant thread on Sec-Iraq forum, by topic: DOS (Thread 1, Thread 2, Thread 3, Thread 4, Thread 5, Thread 6, Thread 7), vulnerability scanner (Thread 1), IP address obfuscation (Thread 1, Thread 2), port forwarding (Thread 1, Thread 2).

[50] The browser appears to have been written from scratch in a Visual Basic-like language and not a fork, or adaptation, of a major open-source browser such as Firefox or Chromium, judging from the visual appearance, feature set, and extent of customization. This might indicate an insufficient knowledge of computer programming on the part of al Nemr to be able to work with large, complex code bases.

[51] A botnet is a network of computers that are linked together and which can collectively perform some task. These networks have some legitimate applications, but can also be wielded by a hacker to launch large-scale attacks, such as a distributed denial-of-service (DDOS) campaign. Constructing a botnet requires compromising a large number of systems and infecting them with malware, called bots, to control the system thereafter.

[52] Al Nemr and the FIE alleged to have penetrated the websites of the Kuwaiti army, the Ministry of Defense of Saudi Arabia, the President of the United Arab Emirates, the US Department of Education, the US Marines, the US Congress, the Czech Army, and Google, among others. The proof for most of these attacks was presented via YouTube videos that are no longer accessible; however, there is no independent confirmation of any of them. Double-checking the proof for the lattermost two claims reveals that the FIE in fact targeted http://czecharmy.cz.cc whereas the correct address for the Czech Army is http://army.cz, and its attack on Google was not a hack at all (it involved feeding Google Mobilizer, a service that formats web pages into mobile-friendly versions, a webpage designed to appear as if it had been hacked). It is therefore unlikely that the other hacks were legitimate.