Occasional Papers

Arab Studies

Arabistik

Nr.9

Ed. Rüdiger Lohlker

Institut für Orientalistik der Universität Wien

Oriental Institute, University of Vienna

July 2016

Cyber Caliphate, United Cyber Caliphate et al.

Rüdiger Lohlker

The German weekly "Der Spiegel" recently published an article claiming that the online attacks using the handle "Cyber Caliphate" originated from Russia.[1] Similar claims have been made in 2015 in the aftermath of the attack on the French TV-station *TV5 Monde* in April 2015.

In 2014 an attack on the Syrian media group "Raqqa is being slaughtered silently"[2] critical of ISIS has been reported. The report says ISIS cannot be ruled out as the source of the attack. The assessment of ISIS' ability to engineer such an attack reads as follows:

"**We think there are several features of the malware attack that align with the needs and constraints of ISIS and its supporters in Ar-Raqqah**, more so than other groups, as we understand them. For example:

- The malware beacons location but does not provide RAT functionality.
- The seeding attempts to obtain a ‘private’ Facebook identity from RSS through social engineering.
- The malware exfiltrates to an online e-mail account, thus not requiring the attacker to maintain a command-and-control server online. […]

Little is publicly known about the technical capabilities of ISIS and its supporters; however, reports have begun to emerge suggesting that ISIS is interested in expanding its abilities. In addition, ISIS has reportedly gained the support of at least one individual[13] with some experience with social engineering and hacking: Junaid Hussain (aka TriCk), a former member of teamp0ison hacking team. While Mr. Hussain and associates have reportedly made threats against Western governments, it is possible that he or others working with ISIS have quietly supported an effort to identify the targeted organization, which is a highly visible thorn in the side of ISIS."[3]

Another article says there may be a capability for cyber attacks at a level of propaganda activities, defacing etc, but it is difficult to assess the extent of a possible danger.[4] The alleged Russian connection remains difficult to track and any accessible reliable proofs are not available.[5] The Russian connection is based on the identification of certain malware used by the hacker group SEDNIT.[6] Trying to blame Russia and pointing at a weakness of ISIS to organize advanced

[1] http://www.spiegel.de/netzwelt/netzpolitik/islamischer-staat-cyberattacken-als-werk-russischer-hacker-enttarnt-a-1098249.html (accessed June 18, 2016) (posted June 18, 2016)

[2] http://www.raqqa-sl.com/en/ (accessed July 8, 2016)

[3] https://citizenlab.org/2014/12/malware-attack-targeting-syrian-isis-critics/ and http://www.infosecurity-magazine.com/news/isis-likely-behind-cyberattack/ (accessed July 8, 2016)

[4] https://www.br.de/puls/themen/netz/cyber-terror-is-100.html (accessed July 8, 2016)

[5] http://freebeacon.com/national-security/cyber-caliphate-hackers-not-linked-to-islamic-state/ (accessed July 8, 2016)

[6] http://www.infosecurity-magazine.com/news/russia-pegged-cyber-caliphate/, http://blog.trendmicro.com/trendlabs-

cyberattacks, makes not a convincing case.

We are back

In November 2015 an article in the online version of the *Daily Mail* hinted at an attack on Twitter by the Cyber Caliphate and published a tweet with the simple message of the Cyber Caliphate saying: "We are back".[7] This attack was interpreteted as a retaliation for the killing of the alleged leader of the group, Junaid Hussain[8], a British hacker killed by a US drone attack. After this killing the usual claims after every targeting killing were made, saying the activity of the Cyber Caliphate have declined.

Leaving aside the fact that there are many other hacker groups online claiming affinity to ISIS, we will notice the lack of in-depth information on the activity of the hacker groups affiliated to ISIS. This paper will provide an overview of this activity.

The "SITE Intelligence Group – Dark Web & Cyber Security" has a list of IS-related hacks by several groups including the United Cyber Caliphate (UCC), Kalachnikv Team, and Caliphate Cyber Army.[9]

The merger of several IS-hacker groups in to the larger United Cyber Caliphate (UCC) announce on April 4, 2016[10], caused some interest[11], even a sort of hype when *hackread.com* wrote about the creation "of a mega hacking group by ISIS".[12]

Media interest was guaranteed when ISIS hackers published lists of names including names of people living in the United States[13], Australia, Canada and the United Kingdom – and even Greece.[14]

security-intelligence/operation-pawn-storm-the-red-in-sednit/, http://www.welivesecurity.com/deutsch/2014/10/08/spionage-ring-sednit-nutzt-jetzt-individualisiertes-exploit-kit/ , https://www.alienvault.com/blogs/labs-research/from-russia-with-love-sofacy-sednit-apt28-is-in-town, and http://www.trendmicro.com/vinfo/us/threat-encyclopedia/search/sednit (accessed July 8, 2016)

[7] http://www.dailymail.co.uk/news/article-3308734/ISIS-cyber-caliphate-takes-54-000-Twitter-accounts-Terrorists-hack-social-media-site-spread-vile-propaganda.html (accessed June 18, 2016)

[8] https://en.wikipedia.org/wiki/Junaid_Hussain (accessed June 18, 2016)

[9] https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=697&Itemid=1355 (accessed July 8, 2016); other lists of attacks are easily to be found on ISIS-related *telegram* channels.

[10] https://www.flashpoint-intel.com/news/flashpoint-issues-new-report-demonstrating-advancement-of-isis-organized-cyber-capabilities/ (accessed July 13, 2016)

[11] https://en.wikipedia.org/wiki/Islamic_State_Hacking_Division (accessed July 8, 2016)

[12] https://www.hackread.com/isis-hackers-united-cyber-caliphate/, http://heavy.com/news/2016/06/new-isis-islamic-state-cyber-caliphate-army-hacking-hackers-digital-security-threat-photo-report/ (accessed July 8, 2016)

[13] For an usual reaction to these threats see https://www.bostonreview.net/us/judith-levine-ISIS-hack (accessed July 08, 2016).

[14] http://greece.greekreporter.com/2016/06/09/greek-names-included-on-new-isis-hit-list/ (accessed July 08, 2016)

Assessing Hacking Capabilities

To some extent the IS-hackers operations tend to be "typical of small groups of 'hacktivists': indiscriminate Web defacements, claims of bigger hacks that appear to be based on the work of others, and claims of responsibility for unscheduled system outages."[15]
A recent report assesses the capabilities of ISIS hackers as follows:

"Call for Cyber Recruits: While ISIS has not explicitly attempted to recruit sophisticated hackers, Deep & Dark Web forums can be used as a training ground, allowing ISIS followers with low-level technical and hacking abilities to hone their skills. Deep & Dark Web forums include sections containing both beginner and advanced hacking courses, hacking tools and manuals, as well as ways to communicate with others for support and guidance.

Techniques and Tactics: While it is difficult to assess what techniques, tactics, and procedures (TTPs) ISIS's supporters employ, based on the types of cyber attacks the various pro-ISIS hacking groups have claimed responsibility for, Flashpoint analysts believe pro-ISIS hackers depend on coordinated campaigns, social media, use of malware, and specific technical tools.

Hacking Tools vs. Malware: Pro-ISIS cyber actors are likely to download hacking tools from publicly available sources while also utilizing both off-the-shelf and custom malware."[16]

And another aspect: *al-Jaysh al-khilafa al-iliktruni*, the name of the Cyber Caliphate Army in Arabic, in one post from June 27, 2016, claims that with their help a "cell of spies […] related to the unbelieving alliance" has been discovered, signalling their involvement in offline activities of ISIS.[17]

So what about the Russians? To answer this question we should turn to the activities of ISIS hackes as discernable the now central online platform of ISIS: *telegram*.

and even names from Florida (http://www.nbcmiami.com/news/local/Report-ISIS-Targets-Hundreds-of-Floridians—382357381.html; accessed July 08, 2016)

[15] http://arstechnica.com/information-technology/2016/04/as-us-drops-cyber-bombs-isis-retools-its-own-cyber-army/ (accessed July 13, 2016)

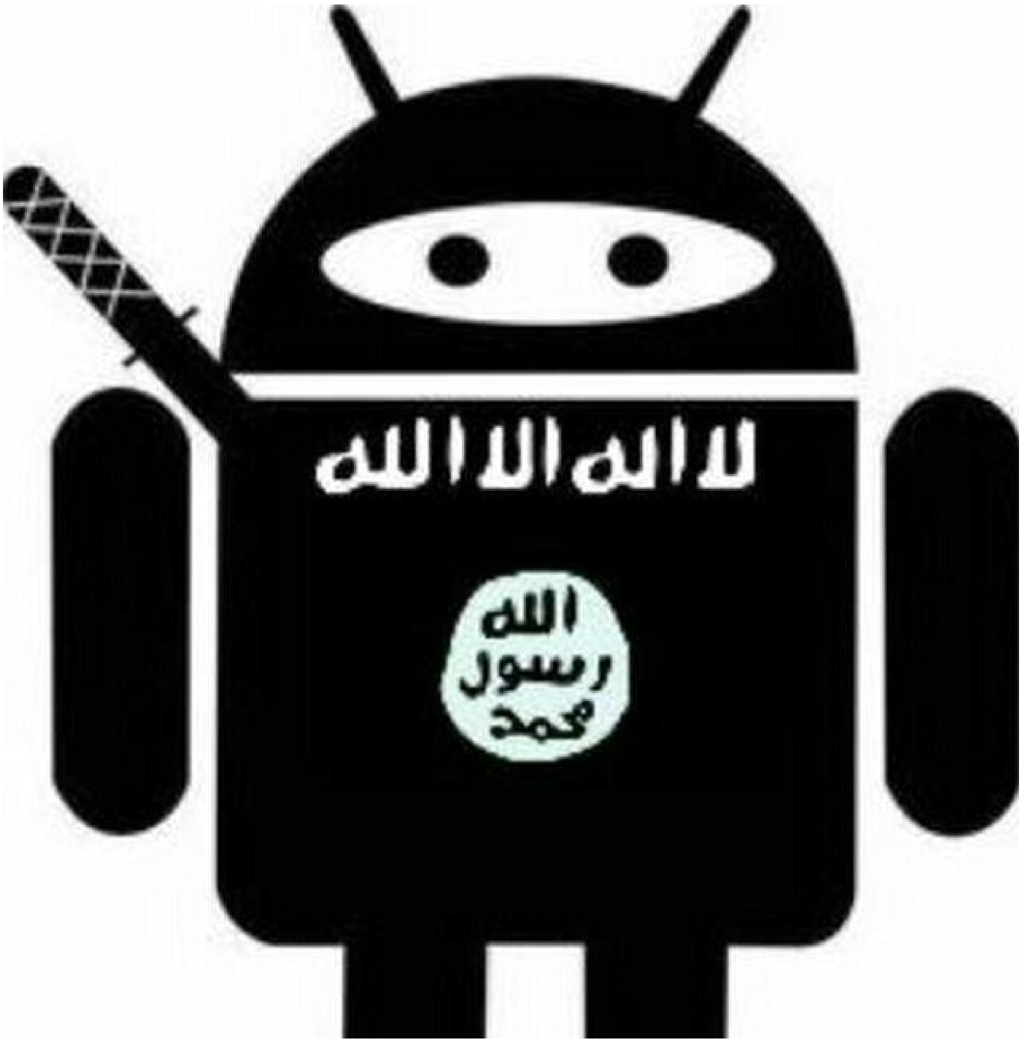
[16] https://www.flashpoint-intel.com/news/flashpoint-issues-new-report-demonstrating-advancement-of-isis-organized-cyber-capabilities/ (accessed July 13, 2016); see also http://www.scmagazineuk.com/uniting-pro-isis-hacking-groups-still-unsophisticated-but-sharpening-skills-report-says/article/492953/ (accessed July 13, 2016)

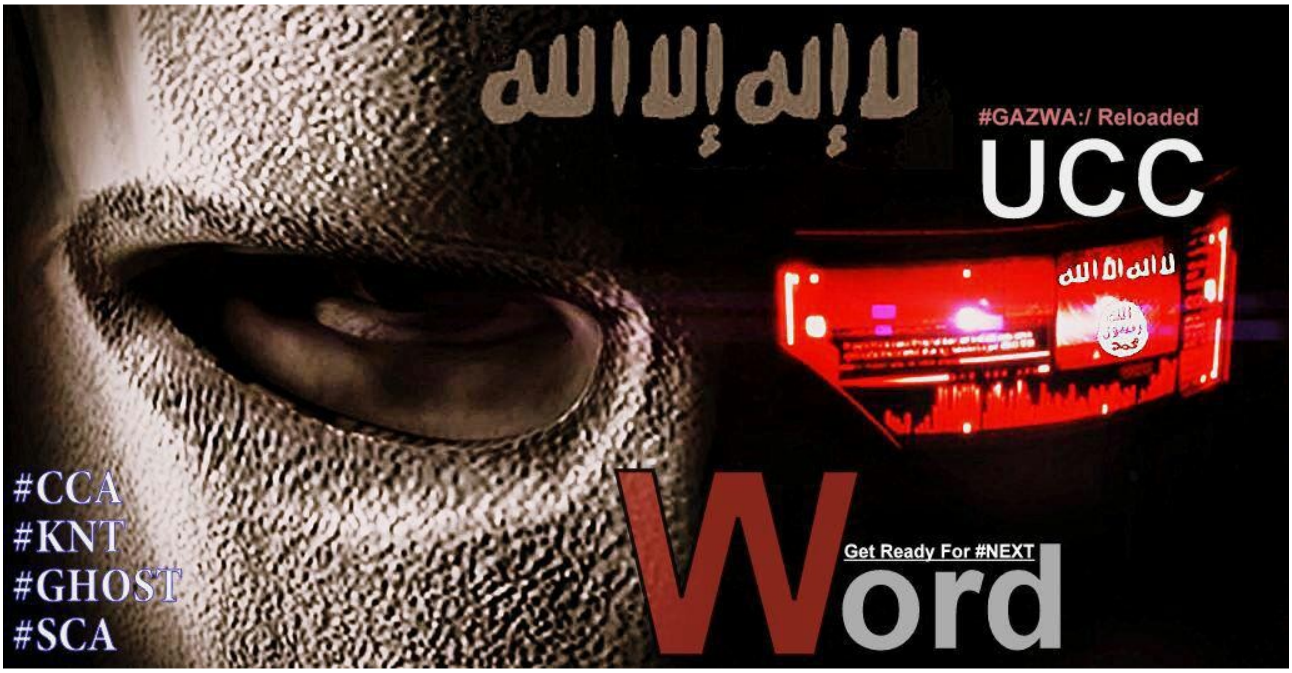
[17] 20:16, channel *al-Jaysh al-khilafa al-iliktruni* (in Arabic) at *telegram.me*.

Telegrams of Hackers

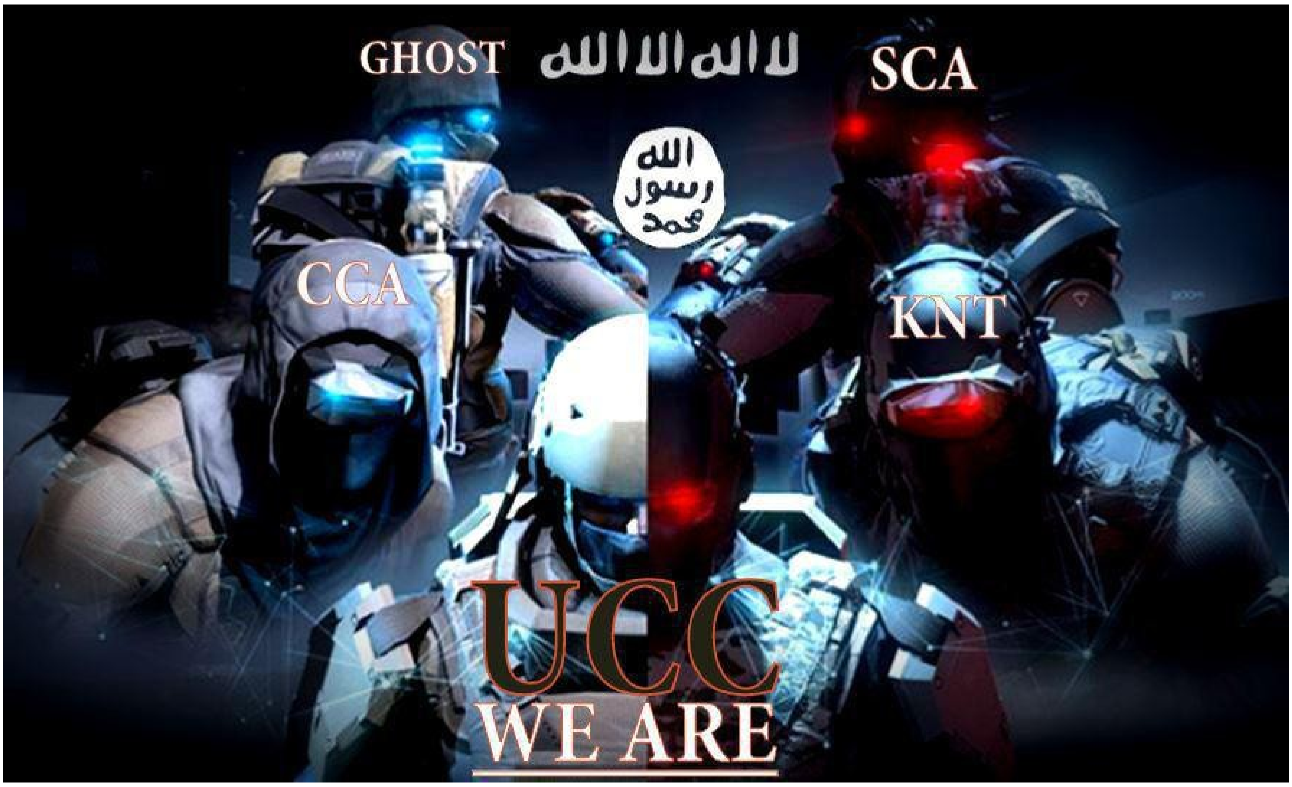
Research on Arabic channels at *telegram* easily discovers a complex activity of this groups activists in the context of ISIS. But at first let us look into the self-representation using some of the graphics created by members of these groups.

Using popular tech-culture





Cyber Caliphate United: Street and gangster coolness



Cyber Caliphate United: Another version of being cool and threatening

Electronic maps on the battlefield

Technical Training

An important aspect of the activities of ISIS cyber activists is providing information to the rank and file members about more secure ways to use electronic devices and media. E. g., they are promoting the use of messenger services like, e. g., *Threema*, said to be more secure than other messenger services.

A whole series of papers deals with the problems of security measures for smart phones discussing all OS available. Other papers discuss vulnarabilities of communication on Internet platforms on a specific level.

The channel *Cyber Caliphate Army (al-Jaysh al-khilafa al-iliktruni*) offers a mix of theological propaganda, military videos and pictures, and other material to be found on other ISIS channels, too. But there is a numbers about international hacks not claiming they were done by ISIS hackers, much more a kind appealing to ISIS hackers to do it themselves.

Apps are offered to return to *Twitter*: "Now, now starts the fight!"

Summarizing this short overview we might say: Although there may have been some Russian influence in the April 2015 – still has to be proven there really was – the ISIS hacker groups and activities are much too complex to be understood by a simple outcry "the Russian".