United Cyber Caliphate

Nadine Liv

ABOUT THE ICT

Founded in 1996, the International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world, facilitating international cooperation in the global struggle against terrorism. ICT is an independent think tank providing expertise in terrorism, counter-terrorism, homeland security, threat vulnerability and risk assessment, intelligence analysis and national security and defense policy.

ICT is a non-profit organization located at the Interdisciplinary Center (IDC), Herzliya, Israel which relies exclusively on private donations and revenue from events, projects and programs.

ABOUT ICT CYBER-DESK

The Cyber Desk Review is a periodic report and analysis that addresses two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse) and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack).

The Cyber Desk Review addresses the growing significance that cyberspace plays as a battlefield in current and future conflicts, as shown in the recent increase in cyber-attacks on political targets, crucial infrastructure, and the Web sites of commercial corporations

Main Findings

1. It seems that that the widespread use of cyberspace by pro-IS terrorist operatives remains within the realm of "use" for terrorist purposes and does not amount to cyber-terrorist attacks. At the same time, it seems that IS supporters on the Internet, such as the FMCC, are striving to develop and improve offensive capabilities. It is possible that the IS does not officially recognize the UCC in light of its low capabilities, but it may claim official responsibility should the UCC carry out a successful cyber-attack.
2. The belief that the UCC plans to carry out a cyber-attack that will pose a significant security threat could explain the assassination of three UCC leaders in American drone strikes. Since their activities were not dedicated to offensive cyber and information security activities, it might be assumed that they were killed for the activities that they carried out on behalf of the IS, including hacking, information security, propaganda and online recruitment.
3. There is a trend of shifting focus to the area of Southeast Asia, as evidenced by the origins of the UCC leaders, the collective's publications, the attack targets and language analysis.
4. It is necessary to distinguish between a virtual protest offense (mainly defacement), which is a *computer* crime, together with its physical counterpart (graffiti), which is a *property* crime, and between the offense of murder. Not everyone who expresses a virtual protest will necessarily kill using cyber weapons, just as not everyone who paints graffiti on people's property will necessarily kill with a weapon.
5. The hacktivism activities of IS supporters have an intrinsic value because they generate the media noise that terrorism aims to achieve in the first place. This position is supported by the fact that the level of cyber-attacks by IS supporters on the Internet has remained low in recent years, while the scope of the groups has increased exponentially.
6. Although hacktivism offenses are minor and do not pose a significant direct threat to security, according to the "broken windows" theory, the key to crime prevention is to focus on minor offenses in order to prevent deterioration and escalation.

Table of Contents

Introduction: Between Electronic Jihad and the Cyber Caliphate

The expression *Electronic Jihad* was coined in 2003 in an article titled, *39 Ways to Serve and Participate in Jihad*, in which Article 34 set down the concept to outline the Internet activity of Islamic terrorist organizations to promote the idea of jihad in cyberspace. Electronic jihad refers to two aspects. The *first* is operative, and deals with incitement and encouragement for the idea of jihad, such as propaganda, financing and media. The *second* is technical, and deals with cyber-attacks and cyber defense.[1] The increase in the number of Internet users since 2003 has led to the creation of a unique culture that is reflected in a variety of exclusive phenomena, such as talkbacks, memes, hacking, shaming and social networks. Habermas refined the term *Public Sphere* as an imaginary or virtual community that does not exist within defined boundaries and is an arena of social life in which public opinion is perfected.[2] In this sense, there is no doubt that the Internet in general, and social networks in particular, constitute the implementation of Habermas's concept. This public sphere has also developed in the Arab world and has provided the younger generation with platforms and mechanisms that enable it to actively participate in public debates, in contrast to the types of regimes common in Arab countries – totalitarian, theocratic or military – which do not grant fundamental freedoms such as freedom of expression.[3] Peter Mandeville maintained that media outlets, and the Internet in particular, will play a significant role among Muslim youth born and educated in the West; youth who seek out spaces and languages in which they can shape an Islam that is relevant to their socio-cultural position and free from the hegemony of traditional interpretation of sources and its control.[4] A clear example of the leveraging power of social networks to reach the masses and bring about change is the Arab Spring.

The Islamic State (IS) terrorist organization is good at harnessing the Internet and social networks — with all their advantages — for the benefit of the organization's needs. This allows terrorist groups to advertise themselves intensively and extensively on these platforms, and to overcome censorship and access information that may have been blocked in commercial media. In addition, the quality of the propaganda material and the ability to distribute it are significant advantages attributed to digital progress.[5] Along with the realization of the electronic jihad concept, a *virtual community* has formed in cyberspace, exercising the public sphere for practical application that deviates from the dual use of the Internet as defined in the 39 ways.

---

[1] As-Sālim, M. B. A. ('Īsā al-'Awshin) (2003–19/5/1424H). *39 Ways to serve and participate in Jihād*. At-Tibyān Publications.
[2] Habermas, J. (German 1962, English translation 1989). The Structural Transformation of the Public Sphere. *Cambridge*, MIT Press 85, 85-92.
[3] Lynch, M. (2006). Voices of the new Arab public. Iraq, Al-Jazeera, and Middle East Politics Today. *Columbia University Press*. New York.
[4] Mandeville, P. (2003). Communication and diasporic Islam: A virtual Ummah? *The Media of Diaspora: Mapping the Globe*. pp 135-148. Editor: Karim, K. H. Routledge. London.
[5] Bertram, L. (2016). Terrorism, the internet and social media advantages. *Journal for Deradicalization, 7*, 225-252.

The two main characteristics of *community*, as described in the academic literature, are the geographical proximity of the members of the community to one other and the ongoing interaction between them. However, in modern times, geographical proximity is not a condition for defining a group of people as a community. An *online community* is a voluntary organization of people based on a common characteristic or interest whose members have continuous interaction on the Internet through various means such as email, forums, blogs, etc. One of the potential functions of online communities is to recruit activists and spur action, especially in cases where the purpose for the which the community is united falls outside the consensus; another function is political polarization and social radicalization.[6]

The Internet, being global and transnational, has the potential to realize the vision of *a unified Muslim community* (Ummah).[7] The virtual caliphate is a distorted version of the historic Islamic Caliphate: a layered community of Muslims led by a caliph who aspire to be part of a country subject to Shari'a while located in the global territory of cyberspace.[8] Winter used the term *Virtual Caliphate* to explain the strategic thinking behind the IS *propaganda* machine through the construction of a theoretical-thematic framework.[9] In January 2017, a team of experts published its prediction that victory on the physical battlefield would not be enough to defeat the IS, and that – in response to its defeat in Iraq and Syria — the organization would likely turn to a virtual safe haven (a 'virtual caliphate') from which it would continue to coordinate and encourage external attacks while building a foundation of support until it will be able to restore its *physical* territory.[10] Nance and Sampson define the virtual caliphate as a '*ghost* caliphate' that will allow the IS to rise after a physical defeat and act as a *cyber-warfare* force.[11]

The Islamic State is not the first to establish a ghost caliphate. There are those who claim that Al-Qaeda was the first guerrilla movement in history to migrate from the physical sphere to cyberspace.[12] For Al-Qaeda, the Internet has become not only a virtual shelter where every dimension of global jihad is taking place online, it has also has created an online jihad university and expanded the potential audience and methods of interaction. The Internet constitutes a *transition* to a functional tool for empowering the media, promoting ideology, recruiting, funding and training activists. For Al-Qaeda, cyberspace serves as its central nervous system.[13]

---

[6] Lev-On, Azi. (2015). *Virtual Communities*. Rassling. (in Hebrew)
[7] Mandeville, P. (2002). *Transnational Muslim Politics Reimagining the Umma. Routledge*. London.
[8] Joseph L Votel, Christina Bembenek, Charles Hans, Jeffery Mouton, Amanda Spencer (2017) Virtual Caliphate: Defeating ISIL on the Physical Battlefield is not Enough. Center for a New American Security (CNAS)
[9] Charlie Winter (2015) The Virtual Caliphate: Understanding Islamic State's Propaganda Strategy. Quilliam
[10] Joseph L Votel, Christina Bembenek, Charles Hans, Jeffery Mouton, Amanda Spencer (2017) Virtual Caliphate: Defeating ISIL on the Physical Battlefield is not Enough. Center for a New American Security (CNAS)
[11] Nance, M., and Sampson, M. (2017). *Hacking ISIS: How to destroy the cyber jihad.*
[12] Magnus Ranstorp (2006) The Virtual Sanctuary of Al-Qaeda and Terrorism in an Age Globalization.
[13] Ibid.

In summary, the conceptualization of the Internet as a potential arena for the implementation of a public sphere for the modern Muslim community has received little attention in the professional literature. Mandeville was the first to identify and formulate the unique potential inherent in cyberspace to "fine-tune" Islam among young Muslims living in the West who seek a collective identity that will, on the one hand, connect them to their heritage and their roots, and on the other hand, adapt to the circumstances of their lives as Muslims living in the "Diaspora" and free them from the chains of the hegemony monopoly of the Ulamā. The connection between the *Muslim-virtual public sphere* and its implementation by a *terrorist organization* focuses mainly on its varying *functional* uses by terrorism as a tool to promote operational needs. Two of the most prominent examples of this are Al-Qaeda, which pioneered the migration to cyberspace, and the IS, which is known for its ability to maximize the features of the Internet to promote propaganda, recruitment and financing with a significant media impact. There is no doubt that the literature investigated these organizations in a comprehensive and extensive manner, but it characterizes the Internet almost entirely as a functional tool for operational needs in relation to the rehabilitation and promotion of activities in the physical sphere. To date, research has not yet been conducted to examine the *cyber culture* of the *IS terrorist organization* and the manner in which the unique characteristics of the IS and its supporters are expressed in cyberspace. Thus, we can point to a unique arrival to the virtual jihadist community — the establishment of pro-IS hacktivist groups. Beyond the Islamic State's functional gain from the Internet, including psychological warfare, publication and propaganda, data mining, fundraising, recruitment and mobilization of activists, networking, exchange of information, planning and coordination,[14] the IS maintains a cyberculture on the Internet.

The working premise of this study is that beyond the functional uses of the Internet by the Islamic State terrorist organization, a unique cyberculture has developed in this sphere. This document investigates the phenomenon of pro-IS hacktivism. It reviews the establishment of several pro-IS hacktivist groups, and then describes the process of the groups' merger into an umbrella organization or collective called the United Cyber Caliphate (UCC). Finally, it offers an assessment of the collective's cyber capabilities.

[14] Weimann, G. (2004). How Modern Terrorism Uses the Internet, *United States Institute of Peace, Special Report.* No. 116.

1. A Review of Pro-IS Hacker Groups

CYBER CALIPHATE (CALIPHATE CYBER ARMY, CCA)

The first pro-IS group is the Cyber Caliphate and it arose immediately with the Islamic State's declaration of the establishment of the Caliphate in the summer of 2014. The group claimed responsibility for the takeover of Newsweek's and CENTCOM's Twitter accounts, and for additional attacks that have garnered widespread publicity. On January 6, 2015, the group launched cyber-attacks against several American targets, including the city of Albuquerque, New Mexico, WBOC News, and more. The group was led by Junaid Hussain (aka Abu Hussain al-Britani), who was born in 1994 and fled Britain to join the IS in 2013 after serving a prison sentence for hacking the email account of former British Prime Minister, Tony Blair. From his residence at an IS base in Raqqah, Syria, al-Britani recruited hackers and nurtured the cyber caliphate that he envisioned until his assassination in an American drone strike in August 2015 in Raqqah, Syria.[15]

During the al-Britani era, cyber-attacks were not as sophisticated as one would have expected from a Western leader, apparently due to al-Britani's inability to provide the IS cyber community with a network of other hackers. The attacks included obtaining unclassified official documents and sensitive information from law enforcement agencies. The information may have been stolen from email correspondence, and not necessarily through hacking, but the group demonstrated at least a basic level of hacking ability.[16]

After al-Britani's death, Siful Haque Sujan, a businessman of Bangladeshi origin and a computer expert who studied and was educated in Britain, became leader of the group. He was also killed in a targeted drone strike in Raqqah on December 10, 2015.[17] Al-Britani's wife, Sally Jones (aka Umm Hussain Britaniya) continued his legacy and became known for her prominent presence on social networks as a recruiter and propagandist for the IS; Jones was declared a terrorist by the UN[18] and was apparently killed in a US drone strike, although the report could not be verified.[19]

---

[15] Alhouri, L., Kassirer, A., and Nixon, A. (2016). Hacking for ISIS: The emergent cyber threat landscape. *Flashpoint*. https://fortunascorner.com/wp-content/uploads/2016/05/Flashpoint_HackingForISIS_April2016-1.pdf. Accessed 04.12.2017.
[16] Ibid
[17] Ibid
[18] UN, (28.09.2015). Security Council Al-Qaida Sanctions Committee Adds Names of Four Individuals to Its Sanctions List. http://www.un.org/press/en/2015/sc12059.doc.htm
[19] MacAskill, E. (12.10.2017). British ISIS member Sally Jones 'killed in airstrike with 12-year-old son'. *The Guardian*. Available online at: https://www.theguardian.com/world/2017/oct/12/british-isis-member-sally-jones-white-widow-killed-airstrike-son-islamic-state-syria Accessed 06.12.2017

Screenshot from Twitter (Source: Unknown)

ISLAMIC STATE HACKING DIVISION (ISHD)

The group arose in early 2015 and seems to be loosely connected to the CCA on the basis of al-Britani's leadership.[20] On October 25, 2015, federal prosecutors revealed a criminal case in which Ardit Ferizi, a Kosovo citizen known as Th3Dir3ctorY and considered the leader of a hacking collective called Kosova Hackers Security, was accused (October 6, 2015) of providing material support to the IS, computer hacking and identity theft violations as a result of the theft and distribution of Personally Identifiable Information (PII) of US service personnel and federal government employees. The Assistant District Attorney in the case said the incident represents the first time that national cyber security has faced a real threat from the combination of terrorism and hacking. Ferizi pleaded guilty on June 15 and was sentenced to 20 years in prison; he admitted that he had obtained administrator privileges for the hosting server of a US company site. The database of the company included the personal information of tens of thousands of the company's clients, including military and government personnel, 1,300 of which Ferizi transferred to al-Britani, who in turn published it as a killing list by sharing a "tweet" on Twitter from an account called the Islamic State Hacking Division (ISHD).[21] The following was written in the document containing the list:

> *"We are in your emails and computer systems, watching and recording your every move, we have your names and addresses, we are in your emails and social media accounts, we are extracting confidential data and passing on your personal information to the **soldiers of the khilafah**, who soon with the permission of Allah will strike at your necks in your own lands!".*

The fact that al-Britani once again shared a tweet from the Islamic State Hacking Division Twitter account means that there is at least a connection between the two groups, the CCA and the ISHD, and perhaps even partial or full overlap of activists under both organizational names. If there is dual

[20] Alhouri, L., Kassirer, A., and Nixon, A. (2016). Hacking for ISIS: The emergent cyber threat landscape. *Flashpoint*. https://fortunascorner.com/wp-content/uploads/2016/05/Flashpoint_HackingForISIS_April2016-1.pdf . Accessed 04.12.2017.
[21] Department of Justice, (23.10.2017). ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison. https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison

Presentation of ICA members (Screenshot from video)

activity by the same players, then there is meaning behind the groups' name selection. Thus, the name of the first group (CCA) reflects advanced conceptual thinking based on a vision for the establishment of a cyber caliphate, while the name of the second group (ISHD) reflects the unique purpose of a division that works for the benefit of the IS in cyberspace. The distinction is significant because the hacking division (ISHD) is a functional tool designed to serve the IS unlike the Cyber Caliphate (CCA), which is an end in and of itself — the establishment of caliphate in cyberspace and its subordination to Shari'a as interpreted by the IS.

ISLAMIC CYBER ARMY (ICA)

The first official statement by the group calling itself the Islamic Cyber Army was first published on September 10th 2015 on Twitter, calling on hackers to join a campaign against the Americans and their supporters, and to support the Islamic State.[22] The statement reads:

> *"The hackers Supporters of the Mujahideen configure under the banner of unification in the name of Islamic Cypher Army to be God willing, working front against the Americans and their followers to support the ISLAMIC STATE Caliphate with all their forces in the field of e-jihad."*

Near the anniversary of the 9/11 attacks, the group launched a propaganda campaign posting on Twitter under the #AmericaUnderAttack and #IslamicCyberArmy hashtags, under which threats were made regarding a cyber-attack and a count-down to a zero hour, along with lists of email addresses of 300 FBI agents and what appeared to be a leaking of passwords into their accounts. Later on, it became clear that the list was taken from a list stolen by the LulzSec hacker group and was not the result of the ICA group's hacking capabilities.

In addition, the group distributed a 10:31-minute video detailing its members, making threats against the United States, and displayed screen shots of sites that the group allegedly corrupted,[23]

[22] Alhouri, L., Kassirer, A., and Nixon, A. (2016). Hacking for ISIS: The emergent cyber threat landscape. *Flashpoint*. https://fortunascorner.com/wp-content/uploads/2016/05/Flashpoint_HackingForISIS_April2016-1.pdf . Accessed 04.12.2017.
[23] https://videopress.com/v/MQXux6re

including the site of the Azeri Amraha Bank and the Iraqi Ministry of National Infrastructures. The video also claimed that the organization had obtained personal information of White House employees. The detailing of the group members also included HACKER ALDMAR.

The detailing of the group members also included HaCker AldMar who in September 2015 posted on Twitter a threat to attack US banks and government sites on September 11th 2015. In response, the FBI issued a report in which it identified HaCker AldMar as a member of the ICA group, and the threat defined by the FBI was harm to government, banking, and military related networks. The ICA group is ranked in the report as having unsophisticated attack capabilities, whose members will seek to exploit opportunities based on technical weaknesses rather than high-level offensive capabilities.[24]

RABITAT AL-ANSAR

Rabitat Al-Ansar is a group that is part of a wider pro-IS hackers' collective called Media Front, which includes, amongst others, Al-Ghurab, Al-Wafa, Al-Minhaj. In this framework, the group operated first as a unit for the dissemination of jihadist propaganda for the IS, and with the expansion of the community of supporters who carry out hacking operations under the name IS, Rabitat Al-Ansar also began claiming responsibility for the hacking operations.[25] In March 2015, the group announced that it intends to launch an anti-American terror campaign under the hashtag #WeWeillBurnUSAgain. The campaign included the distribution of propaganda supporting the IS in English, including videos showing operational activity against US forces in Iraq, the decapitation of US citizens, and messages from bin Laden and other prominent al-Qaeda leaders directed at the United States. In April, the group issued a statement claiming responsibility for the theft of personal information of 2,000 people, most of them Americans, and others Canadian, Norwegian and Australian citizens, and even released a sample of 400 of them to prove the reliability of the information, but it was not clear whether the information was stolen through hacking or whether it was gathered from open sources online.[26] In response, the FBI investigated the threat and published a report that concluded that the cyber-attacks the group took responsibility for were actually old attacks that had already been solved. According to the report, if the group carries out a hacking, it is

[24] Private Industry Notification. (10.09.2015). Possible September 11 Cyber Threats from ISIL-sympathetic hacking group Islamic Cyber Army. *FBI*. Available online at: https://www.texasbankers.com/docs/FBI_Private_Sector_Advisory_Hacking_Threat_Islamic_Cyber_Army_20150910.pdf. Accessed 08.12.2017

[25] Nance, M., and Sampson, M. (2017). *Hacking ISIS: How to destroy the cyber jihad. p.33*

[26] Alhouri, L., Kassirer, A., and Nixon, A. (2016). Hacking for ISIS: The emergent cyber threat landscape. *Flashpoint*. https://fortunascorner.com/wp-content/uploads/2016/05/Flashpoint_HackingForISIS_April2016-1.pdf . Accessed 04.12.2017.

assumed that this is the exploitation of a known weakness based on a technical opportunity rather than a high capability.[27]

Left: UCC announcement showing Naiyf as the HaCker AldMar ; Right: An article by the Kuwaiti news agency about Naiyf's arrest (source: Telegram)

In May 2015, the group released a video called Message to America: From the Earth to the Digital World. In the video the group declares that its members are the hackers of the Islamic State, and the group is committed to electronic warfare against the United States and Europe, and even threatens that the information security of the West is in its hands, while clarifying that the group will soon dominate the electronic world of the West.[28] In the video, the group boasts of vandalism attacks "signed" by the CCA group, indicating an interplay between the pro-IS hacker groups. In addition to the repetitiveness of the matter of control over the digital world, the video prominently refers to the economic aspect. The group notes in the video that "despite the multi-billion-dollar investment to protect the electronic sites — it has become easier to hack your sites [the US and Europe]."

The two groups, ICA and Rabitat al-Ansar, focus mainly on the *United States*, as evidenced by the publication of propaganda videos explicitly addressing Americans, by the proclamation of campaigns against the United States, the use of the hashtags to disseminate propaganda making explicit threats against the United States, and by setting the anniversary of the attacks on the World Trade Center for the launching of expansive campaigns. The entity HaCker AldMar was finally identified as Uthman Zein Al-Naiyf, a Kuwaiti citizen arrested for disseminating pro-IS content on

[27] Private Industry Notification, (22.05.2015). May 2015 Cyber Threats from Extremist Media Group Rabitat al-Ansar. *FBI*. https://www.ccroc.us/wp-content/uploads/gravity_forms/10-a04158748a963f24f77eba5229696b32/2015/06/FBI-Private_Industry_Notification-May-2015-Cyber-Threats-from-Extremist-Media-Group-Rabitat-al-Ansar.pdf?TB_iframe=true

[28] https://www.liveleak.com/view?i=42f_1431453135

the Internet. By virtue of his association sometimes as a subgroup of Rabitat Al-Ansar and sometimes as an individual member of the ICA group, it is possible to infer the flexibility and liquidity of the groups' array. At the very least, the groups are connected to each other and another reasonable possibility is that these are groups that share member/s or that this is a single group with dual branding. Another finding that may support this conclusion is the fact that there is no hacker with high offensive capabilities, even when there is an alleged claiming of responsibility on the part of the hackers for hacking actions with security or financial significance, that later turn out to be a hoax, which transfers the center of gravity of the hacktivist activity from an offensive ability to mere dissemination of propaganda.

SONS CALIPHATE ARMY (SCA)

Mention of this subgroup was first observed in January 2016 in the CCA's publication[29] of a video titled "Flames of Ansar", which claimed responsibility for the hacking of 15,000 Facebook and Twitter accounts (10,000 Facebook accounts, 150 Facebook groups, 5,000 Twitter accounts), and threatening the lives of the companies' founders, Mark Zuckerberg and Jack Dorsey, if they do not stop removing accounts associated with ISIS from their systems. At the very least, the publication attests to a close connection between these two groups; Similar to ISHD, here too the group's source is associated with the CCA.

Interim summary

With the declaration of the IS organization on the establishment of the Islamic Caliphate, al-Britani conceived and nurtured a vision of a cyber caliphate. He set up the first pro-IS hacker group CCA. Although the organization is not regulated by a hierarchical leadership, and despite the sporadic nature of the actions, this is not an anarchist entity such as Anonymous. Al-Britani entered, on his side, into a relationship with two other pro-IS groups – ISHD and SCA. The ISHD group is responsible for leaking personally identifiable information (PII), representing the first time that a real threat to national cyber security was posed by hacking and terrorism. Although the SCA group has not reached the level of attack capability that poses such a threat, its claim to the founders of Facebook and Twitter suggests that the social networks serve as a tool of the utmost importance for the group. Because the video that was published has a low level of graphic editing, it is not propaganda that the members of the group see before them, but rather the hacking operations into user accounts per-se. Although the group does not have a high level of offensive capabilities, there is no doubt that a desire to develop such capabilities was expressed and a working assumption

[29] Nance, M., and Sampson, M. (2017). *Hacking ISIS: How to destroy the cyber jihad.* p. 27

should be made that this is a matter of time before it acquires education and more advanced offensive tools.

The ICA and Rabitat al-Ansar focus on the videos that were published and the campaigns launched by the United States. Rabitat Al-Ansar has become an organization that specializes in disseminating propaganda through media channels, controlling the digital world and harming the economic sector. The group underwent a change and from a propaganda distribution unit it has changed its character to an offensive group that seeks to harm mainly information security and the economic system. Despite the distinction in the required technical skills, the focus on information and economics undermines the foundations of American values and therefore maintains a propaganda aspect. The HaCker AldMar entity is sometimes identified as a subset of the Al-Ansar Rabitat and sometimes as an individual member of the ICA group, and it is possible that the two options coexist, hence the flexibility of the groups' array and the inconsistency in their branding.

The question of conceptualization of the cyber caliphate arises. Is this a functional tool intended to serve the IS, like any other operational use that the terrorist apparatus channels in its favor, or is this an end in itself – the establishment of caliphate in cyberspace and its subordination to the Shari'a as a concept shaped by the younger generation; A generation educated on smartphones and video games. On the one hand, it should be remembered that the IS organization never formally declared a "digital army", and on the other hand, if the IS organization was opposed to the activities of its hacker supporters, it would probably have expressed an opposition that in turn would have put an end to their activities; The IS abstention from responding in this matter constitutes tacit agreement. Just as the IS does not claim responsibility for any physical attack (not in cyberspace) because it must meet the standard of success and reliability in order to be worthy of the support of its loyal audience, it is quite possible that the reason for the fact that no responsibility was claimed for cyber-attacks is because these attacks are not yet mature enough to conform to the IS standard, in its cyber counterpart. If we accept this conclusion, and assuming that the hacker groups indeed strive to improve, then the way to claim responsibility for a cyber-attack on the part of IS, is a matter of time.

2. Unification of Pro-IS Hacker Groups

UNITED CYBER CALIPHATE (UCC)

In April 2016, the pro-IS hacker groups merged to an umbrella organization called United Cyber Caliphate (UCC); The groups operate in cyberspace as the 'electronic army' of the caliphate. The union was first published on the CCA Telegram channel and announced a union of the groups: Ghost Caliphate Section, Sons of Caliphate Army, Kalachnikov E-Security, Cyber Caliphate Army[30]

The unification banner. Source: ibtimes website

Of the four groups presented in the union, two are known as IS supporters, the Cyber Caliphate Army (CCA) and the Sons Caliphate Army (SCA). The two new groups presented are Kalachnikov E-Security Team and Ghost Caliphate Section.

In said month, the UCC organization claimed responsibility for leaking information from the date of the declaration of union (April 5th 2016), and the publication of such information was usually accompanied by a call to carry out "lone wolf" attacks on the listed targets. The UCC also corrupted sites as part of the #KillCrusaders campaign, from which the United States, Chile, China, France, Malaysia and Mexico were affected. On April 18th 2016, the organization launched the #Gaza_Reloaded campaign, where members of the organization claimed to have leaked personal information of the accounts of 10,000 people. A few days later (April 21st 2016) the organization published a hit list of New York residents together with a banner stating that they want these people

[30] Russon, M. (05.04.2017). Isis cyber army grows in strength as caliphate hacking groups merge on Telegram. *IBTIMES.* http://www.ibtimes.co.uk/isis-cyber-army-grows-strength-caliphate-hacking-groups-merge-telegram-1553326

dead; Later on (April 24th 2016) the organization published a list of US State Department employees who are also wanted dead.[31]

#OP_GAZ_CHAMBER

The first official campaign of the new united organization under the new leadership of the Osed Agha was launched in December 2016 under the name "#Op_Gaz_Chamber", and it emphasizes the continuation of its activity against the "enemy targets" in the cyberspace while harshly criticizing the Saudi regime for its cooperation with Western forces. The group reported on its Telegram channel that it managed to break into Saudi servers and steal personal data of soldiers, which it threatened to reveal. The group later issued a statement calling for the assassination of the "Saudi group", in which a $ 5,000 reward was placed over each soldier. This refers to 55 Saudi security personnel whose identity was exposed through a series of photographs following the statement.

Left: an invitation to carry out a hit; On the centre and right: two photos from the hit list (source: Telegram)

#DEMOLISHING_FENCES

A second official UCC campaign was launched in January 2017 under the name "#Demolishing_Fences", characterized by attacks on private networks and support for lone wolf attacks. Later, in February, another hit list of 4,000 names was found on the laptop of one of the IS recruits from West India who was caught and arrested. The list included personal details of professionals perceived as threatening the organization's ideology. The list included computer specialists from around the world employed in commercial companies such as Amazon, Intel, Exxon, BMW.[32]

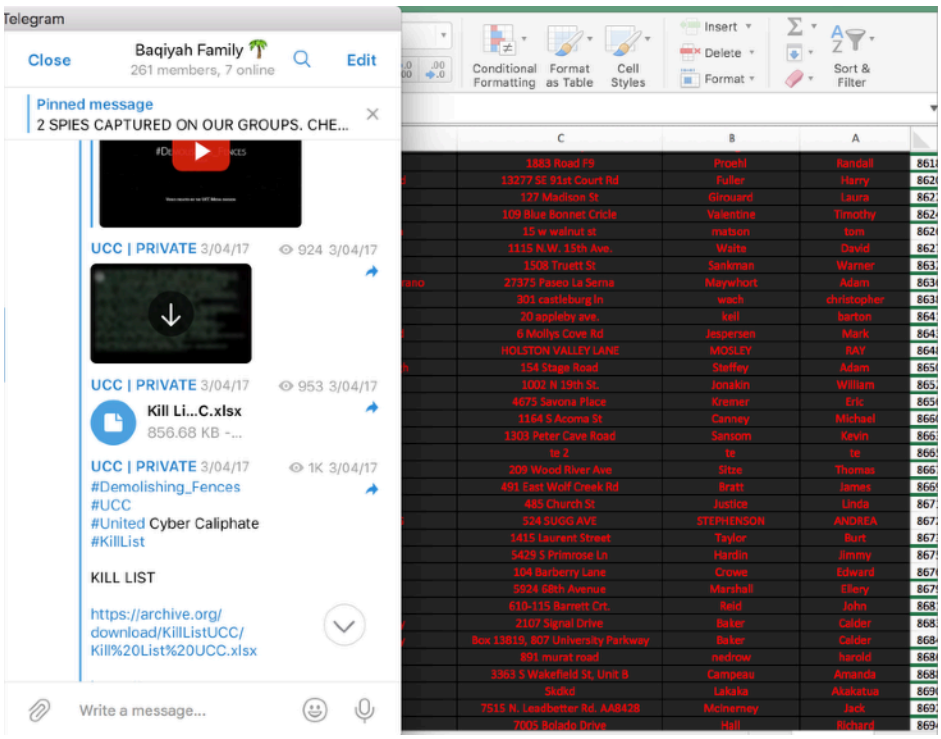
[31] Nance, M., and Sampson, M. (2017). *Hacking ISIS: How to destroy the cyber jihad.* p. 27
[32] Pagani, D. (09.02.2017). India: Counter-terrorism investigators probe IS kill-list with names of many IT professionals. *WION*. http://www.wionews.com/south-asia/india-counter-terror-investigators-probe-is-kill-list-with-names-of-many-it-professionals-12216

On March 16th, the group released a video in which it announced the death of Osed Agha, the group's leader, in a US air strike. Agha is identified as being responsible for the distribution of hit lists. In response to the elimination, the UCC produced, at the end of March 2017, a recruitment video according to which the group faces a new stage in the struggle against "the countries of heresy" and electronic armies. The campaign will focus on attacking private networks and supporting physical attacks of "lone wolves". The video opened with a tribute to Agha, showing the group's achievements in the first campaign under the leadership of Agha, which include, according to the UCC, the hacking of sites, some of them of Iraqi politicians, of hundreds of social media user accounts and surveillance cameras. The group also claims that it managed to crash six sites through a DDoS attack and distribute three hit lists. Later in the video, the new leadership is presented with three branches — Cyber Kahilafah, Kalashnikov Team and Sons of Caliphate Army. The new structure includes four divisions: Ghost Section, Katibat al-Khansaa, Liwa al-Guraba and UCC Media Front. At the end of the video, the group calls for the recruitment of additional hacker groups to its ranks.[33]

Screenshots from the tribute video to Agha showing the UCC organizational structure (Source: Cyber Desk)

In April 2017 an additional hit list of 8,786 people was distributed. The list was distributed in an Excel file using closed Telegram channels and accompanied by a video for verification. The video opens with a threat to the American people and President Trump. A written statement is issued stating that the IS will continue to attack the American people and that the UCC will begin a new phase in the war, called *Demolishing Fences*. A message is then displayed announcing the distribution of a list of more than 8,000 people with their names, addresses and email addresses, and the viewers are asked to kill them wherever they may be. In the next scene, an execution is documented using the IS modus operandi, along with a presentation of the first 200 names on the list (see images on the next page).

33 Cyber Desk a, (01.05.2017). Cyber review no. 21. *International Institute for Counter Terrorism (ICT)*. https://www.ict.org.il/Article/2097/cyber-review-no-21#gsc.tab=0



A screenshot of the hit list and the Telegram group in which it was published

CYBER KAHILAFAH

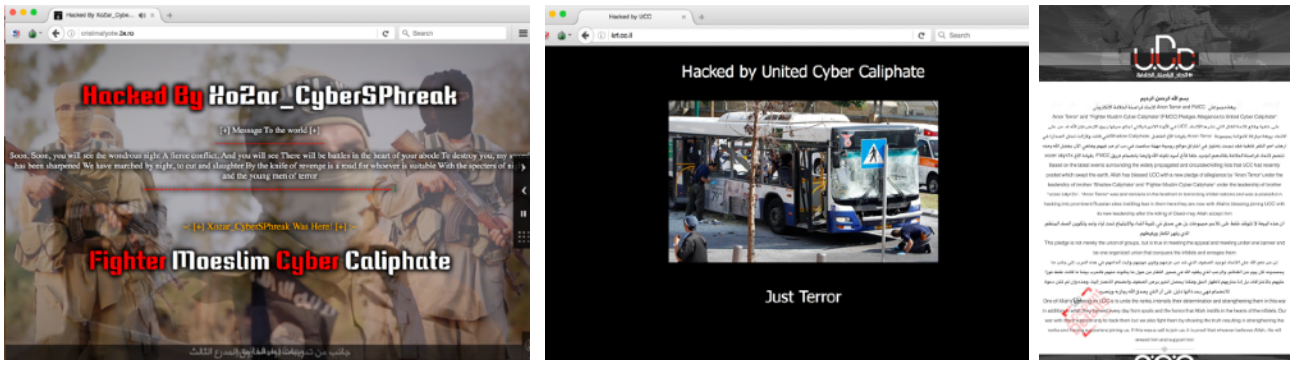
On June 23rd 2017, the Cyber Kahilafah group announced on its Telegram channel the establishment of the group's onion website. The site is on the DarkNet, it is not accessible by conventional browsers such as Google Chrome or Internet Explorer and is not indexed in search engines. As of December 23rd 2018, the site is inactive. In addition, the group also established a Telegram channel on this date.

Top: The Telegram Channel

Left: the onion website URL. Source: Telegram

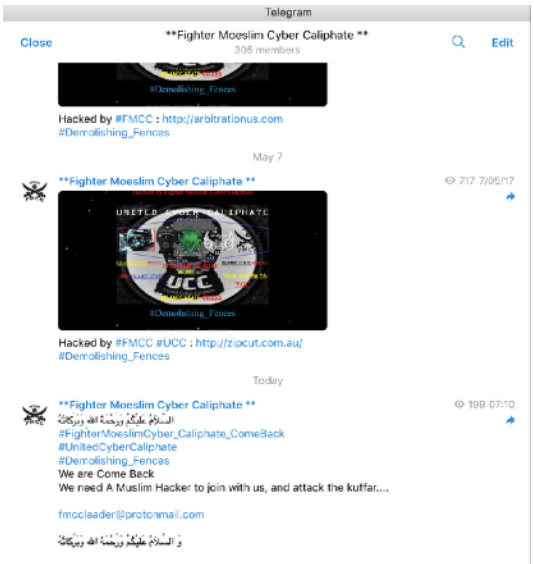
FIGHTER MOESLIM CYBER CALIPHATE AND ANON TERROR

On April 11th 2017, the UCC has two other hacker groups join its ranks, Anon Terror, led by Shadow Caliphate, and Fighter Moeslim Cyber Caliphate (FMCC), led by Xo2ar CyberSPhreak. After the announcement, a wave of vandalism attacks was launched against many sites on which the hackers left their mark and group affiliation; This is the accepted practice of joining the organization, and on some sites a message was left saying that the site will be monitored.[34]



Left and center: sites that were defaced in the wave of cyber-attacks; Right: The announcement from the Telegram channel.

On May 25th 2017, the FMCC group posted on its Telegram channel that it was looking for another Muslim hacker to join its ranks to attack the infidels. The post was accompanied by an encrypted email address (Protonmail) for contacting the group leader anonymously.



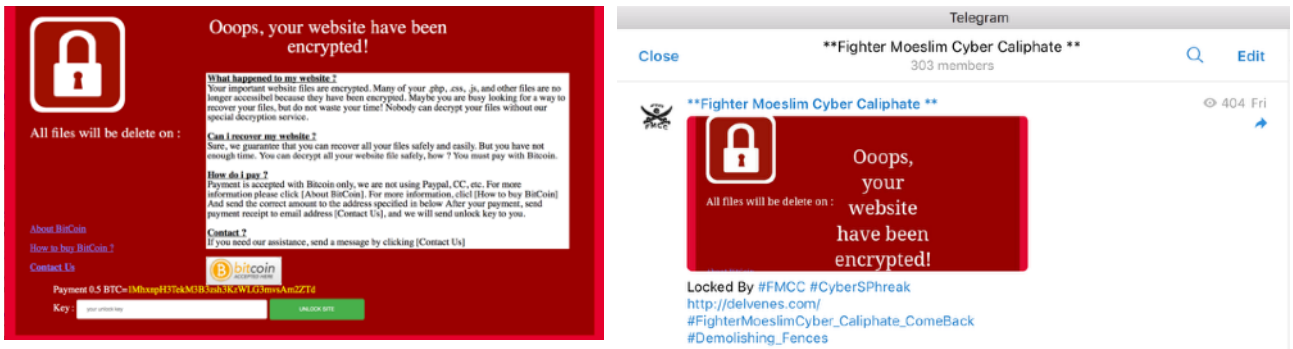
From the FMCC Telegram channel

[34] Cyber Desk a, (01.05.2017). Cyber review no. 21. *International Institute for Counter Terrorism (ICT)*. https://www.ict.org.il/Article/2097/cyber-review-no-21#gsc.tab=0

In this context, it should be noted that in April 2017, the Mujahidin Cyber Army (MCA) hacker group, of Indonesian origin, identified with al-Qaeda, ridiculed on its Telegram channel the FMCC's poor capabilities; This is another niche in which the rivalry between Al-Qaeda and ISIS is expressed.

A screenshot from the MCA Telegram channel

On May 26th 2017, after the extensive Wannacry cyber-attack that took place in early May 2017, a screen shot depicting the Wannacry the cyber-attack, which is essentially a copy of the ransomware Wannacry, was uploaded to the Telegram channel of Fighter Moeslim Cyber Caliphate (FMCC). The attacked site was geographically linked to Jakarta, Indonesia. This attack is unique because the choice to use the technical means of ransomware is a deviation from the group's modus operandi. The group usually corrupts sites, and through this virtual vandalism, it sends ideological messages expressing support of the IS. On the other hand, said attack did not focus on disseminating ideology, but on the intention of generating economic profit. It should be borne in mind that the use of ransomware for terrorism has a double potential advantage – both generating economic profit to finance the terrorist activities and causing economic harm to the site owners, which coincides with the spread of the IS towards East Asia in May 2017 (an extensive discussion can be found below).[35] An examination of the Bitcoin Wallet on December 23rd 2018 revealed that it was not used.

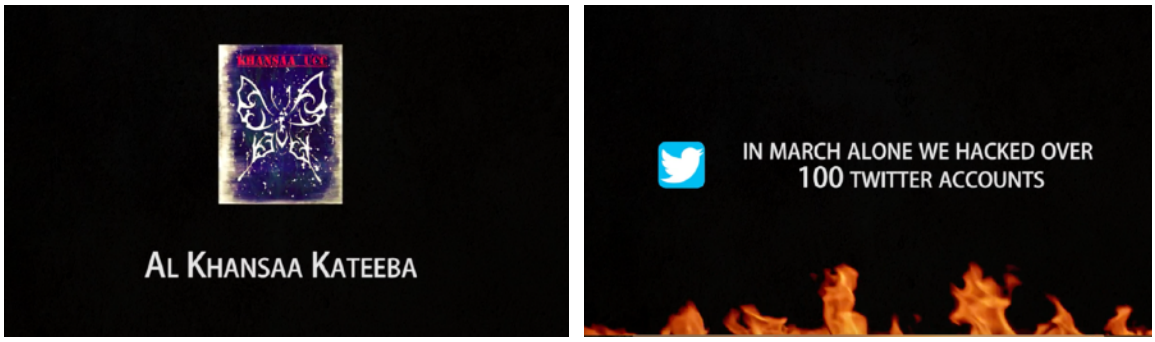


Left: screenshot of the site being attacked ; Right: a screenshot from the closed Telegram channel of the FMCC group

[35] ICT Cyber report no. 22, p. 27: https://www.ict.org.il/Article/2110/cyber-report-no-22-june-august-2017#gsc.tab=0

AL KHANSAA KATEEBA

On April 15th 2017, the UCC published a video showing Al Khansaa Kateeba as the organization's first women's division. In the video, the division is presented as being in charge of hacking into the social media accounts of the infidels and the "spamming" of their accounts in order to disrupt their communication. It is also alleged that in March alone, the division broke into more than 100 Twitter accounts. However, an examination of the hacked accounts shows that these accounts are not maintained, which may indicate that they were chosen because they are an easy target.[36]



Screenshots from the video presenting Al Khansaa Kateeba

THE CYBER CALIPHATE ARMY (CCA) CHANGES ITS NAME TO THE CYBER CALIPHATE TERRORISM ARMY (CCTA)

The Cyber Caliphate Army (CCA) has issued an official statement (March 8th 2017) regarding the changing of its name to the Cyber Caliphate Terrorism Army (CCTA). The statement said that the change was due to a request submitted by the UCC to the CCTA because of the similarity in the group's previous name to one of the UCC divisions; The CCTA's acquiescence is a testament to the good relations between the different groups. Thus, the CCTA group continued to hack into social media accounts and corrupt them and upload to the group's Telegram channels screenshots of Facebook accounts that were hacked with their signatures, indicating that the one responsible is the CCTA group. Examination of the accounts that were compromised revealed that these accounts are not maintained on an ongoing basis and it can be assumed that they were chosen as targets for the attack because of the relative ease with which they can be attacked.[37]

[36] Cyber Desk a, (01.05.2017). Cyber review no. 21. *International Institute for Counter Terrorism (ICT)*. https://www.ict.org.il/Article/2097/cyber-review-no-21#gsc.tab=0

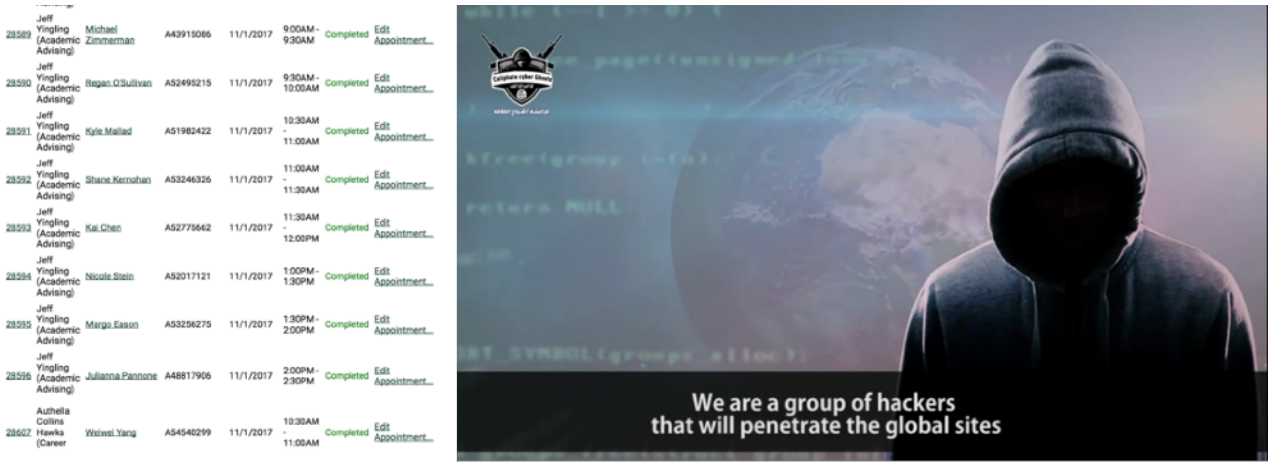
[37] Cyber Desk b, (11.05.2017). CCTA's statment regarding the end of the raid of al-'Adnani. *International Institute for Counter Terrorism (ICT)*. Available online at: https://www.ict.org.il/Article/2000/CCTA's-Statement-Regarding-the-End-of-the-Raid-of- al-'Adnani#gsc.tab=0

On May 10th 2017, the group issued an official statement announcing the end of the operation in the name of the IS spokesperson, Abu Muhammad al-'Adnani, who was killed on August 30th 2016. The statement claimed that the operation focused on social media from three aspects: *first*, closing the accounts of Rafidi (a derogatory name for Shiites) and heretics by reporting these accounts as containing inappropriate content such as nudity. The group declared that 1,843 pages have been closed and removed from the network. *Second*, hacking into Facebook pages of heretics and their defacement. The group declares that 376 pages that were hacked. *Third*, targeted hacking of Facebook pages, especially against spies. The group later thanked all the soldiers who took part in the work and its members asked that Allah consider the achievements of their work. Finally, the group asks all soldiers to participate in the next operation, which will be published soon. The group's Telegram channel posted screenshots to prove said hacking to the Facebook accounts. At least 20 different users contributed to the collaborative effort and transferred such images for public sharing by the group operators. In a sample examination of the hacked accounts, it was found that one account, whose owner publishes content in English and Hindi, has 76 "friends"; Another account had 12 "friends", some of Bengali origin; And at least two other accounts with names of American/ English origin are completely empty – with no profile picture, no publications, and with no "friends". There is no doubt that the level of hacking is very basic and relies on the ease of hacking and not on the ability of hackers. It is not inconceivable that at least some of the accounts that the group declared to have hacked are actually fictitious accounts created in order to place the group's "signature" on them, thereby giving the group credit for a hacking that did not occur.

Screenshots from Telegram groups. Center and left: Accounts that have been defaced; Right: Declaration on change of name; Source: Telegram

CYBER CALIPHATE GHOSTS

The pro-IS hacker group, Cyber Caliphate Ghosts, has released a video in which it announces an electronic war against the crusader countries fighting against the IS. The first to be identified as targets for cyber-attacks are *military and government sites*, and it has been made clear that the hackers aim to damage *infrastructure* and leak *personal information*. In the subsequent publication, a list containing information on 17,487 personal meetings between students with academic advisors, that was stolen from the *University of Michigan*, was posted on the Telegram channels. The list does not disclose personal information of the individuals in it, but it does indicate the ability to hack into the databases of an academic center, as opposed to the prevalent defacement attacks. It should be noted that this is not the first time that the University of Michigan site has been hacked. On November 2016, hackers entered the university's databases and stole personal information of students and faculty members that included names, social security numbers, and dates of birth, and the information was leaked on the internet.[38]



Left: A screenshot of the Michigan University list; Right: screenshot from the Caliphate Cyber Ghosts video. Source: Telegram

TEAM SYSTEM DZ

The pro-IS hacker group, Team System DZ, hacked the servers of a company hosting sites of *schools in New Jersey* and uploaded to the sites propaganda videos encouraging recruitment to the IS. The cyber-attack lasted about two hours, during which the sites posted IS propaganda videos through YouTube uploads. It is believed that no personal information of students or staff was leaked

[38] https://www.forbes.com/sites/leemathews/2016/11/19/michigan-state-university-hacked-student-data-stolen/#28b4b8e54483

and that the attack amounted to defacement and propaganda; The case was transferred for investigation by the FBI (November 7th 2017).[39]

The group posted on its Telegram account a video and a number of banners threatening with the launching of an electronic attack on December 8th 2017 against the coalition countries participating in the war against the IS, *especially against the United States*. According to it, its friends managed to hack into classified websites of the US Army, the Ministry of the Interior, the State Department and other offices and steal great quantities of classified material. The group added that it intends to publish some of the stolen information and send the rest to single terrorists so they assassinate the individuals mentioned in the list and so as to intensify the scope of the attacks. In the concluding remarks, the group stressed that the IS would eventually defeat its enemies.

ANSHAR CALIPHATE ARMY (ACA)

In June 2018 another group called Anshar Caliphate Army emerged, identifying itself as part of the UCC collective. Although most of the hacktivists do not expressly refer to themselves as hacktivists, and the term used primarily by information security professionals,[40] the group identified itself as hacktivist. The group was recorded in closed Telegram groups and language analysis revealed that the group was Indonesian.

An ACA poster

[39] http://www.nj.com/essex/index.ssf/2017/11/hack_posts_isis_recruitment_video_on_nj_school_web.html
[40] Dorothy Dennings (08.09.2015) The Rise of Hacktivism. Georgetown Journal of International Affairs. Available at: https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism Accessed December 3, 2018.

#OPTHEWORLD

On July 27th 2018 the Anshar Caliphate Army group published a poster detailing the cyber-attacks it claims to have carried out in May to July 2018 under Operation #OpTheWorld. Thus, it detailed 160 sites that were corrupted in a defacement attack; 110 Facebook accounts that were hacked; 20 Instagram accounts that were hacked. The attacks targeted websites and accounts from a variety of countries: India, Canada, Russia, England, United States, Israel, the Netherlands, Germany, France, Brazil, Indonesia, Taiwan and China.

The announcement by the Anshar Caliphate Army

PUBLICATIONS BY THE UCC COLLECTIVE

In September 2017, the UCC Group launched a series of *hacks into user accounts* on social media networks. The hackers uploaded to the group's Telegram channel screenshots to document the hacks. At the same time these user accounts were reported as *violating the terms of use* resulting in their suspension, activity that is also documented and screenshots being uploaded to the group's Telegram channel.

On November 24th 2017, the UCC collective posted a four-minute video in which the group boasts the *hacking* of hundreds of Facebook and Twitter user accounts. The group *leaked* a partial list of user names and passwords of the hacked accounts and according to the video the group also created hundreds of new Facebook, Twitter and Instagram accounts, and the final message is that the UCC has returned to activity and that "we will make your sites a tool to our media". The group's Instagram accounts have been in existence for a long time, but use of the platform has recently

increased because of the ability to transfer videos (known as "story" on Instagram) that are automatically deleted shortly after they are uploaded. The video is accompanied by subtitles in English and Arabic simultaneously and is edited at a high level.

A screenshot from the UCC video

The United Cyber Caliphate (UCC) hacker group is recruiting new hackers to its ranks. The group constitutes an umbrella group for several hacker groups operating with the support of the Islamic State. A new group was identified in the list of groups that joined the organization, called Islamic Intelligence. For contacting users, the UCC leaders use KEEMAIL.ME email; A service for sending encrypted emails.

Banners posted by the UCC

On July 9th 2018, the UCC collective issued a statement according to which following the attack *on the East Asian countries*, and after 21 days have passed, the Caliphate hackers have hacked into at least 213 websites in Thailand, the Philippines, Indonesia and South Korea. The group also crashed

nearly 530 sites by SoDD attacks. According to the report, more than 700 social media accounts were hacked, most of them belonging to Muslim soldiers who transgressed and crusaders in these areas.

On August 28th 2018, the UCC collective published an infographic, which reported cyber-attacks it had carried out over 70 days, beginning on May 19th 2018 (the third day of Ramadan). The attacks included the crashing of 770 sites by DDoS attacks, hacking and destroying of more than 900 international sites, hacking over 1,500 social media accounts. The groups that participated in the attacks were: Anon Terror, Team System DZ, Islamic Intelligence, Caliphate Cyber Army, Anshar Caliphate Army, Ghost Caliphate Section, Sons Caliphate Army, Fighter Muslim Cyber Caliphate. The infographic was posted on the Telegram channel in Arabic and English, and was accompanied by text saying that *most of the attacks in the infographic occurred in East Asia* and under the #OpTheWorld cyber campaign.

The message posted by the UCC

The UCC collective has been steadily growing since the rise of the first group identified with it, Cyber Caliphate. The group emerged in 2014, immediately after the establishment of the Caliphate, and was led by Junaid Hussain, who was born in 1994 and fled from Britain to join the Islamic State in 2013, after serving a prison sentence for breaking into the email account of former British Prime Minister Tony Blair. From his seat at the IS Al-Raqqah base in Syria, al-Britani recruited and nurtured the cyber caliphate he envisioned, until his elimination by an American drone attack in August 2015 in Al-Raqqah;[41] Since then there has been an increase in the number of active groups

[41] Alhouri, L., Kassirer, A., and Nixon, A. (2016). Hacking for ISIS: The emergent cyber threat landscape. *Flashpoint*. https://fortunascorner.com/wp-content/uploads/2016/05/Flashpoint_HackingForISIS_April2016-1.pdf . Accessed 04.12.2017.

and five years later, the collective is now comprised of about ten groups.[42] Moreover, the case studies above reflect *a trend of increase in the scope of activity of the pro-IS hacktivists in Southeast Asia.* This can be deduced from a language analysis combined with the choice to attack targets in East Asian countries, together with the emphasis in the infographic that most of the attacks took place on the East Asian front.

The infographic published by the UCC

[42] In a publication by the Fighter Moeslim Cyber Caliphate group (FMCC) from July 9, 2018, the following groups are listed: Caliphate Cyber Army, Ghost Caliphate Section, Anon Terror, Fighter Muslim Cyber Caliphate, Sons Caliphate Army, Islamic Intelligence, Anshar Caliphate Army, Al Barra Bin Malik Battalion, Team Systems DZ, Al Siddiq Battalion.

3. Evaluating the Cyber Capabilities of the UCC

In a discussion of cyber terrorism, the distinction between two spheres of use made by terrorism in information technology must be clarified; Terrorist use of computers as a means of assisting their terrorist activities, as opposed to terrorism involving computer technologies as a weapon or a target; When only the latter use falls within the realm of cyber terrorism, while the former, whether for purposes of propaganda, communication, or other purposes, remains "use".[43] The IS organization exploits cyberspace for the use of modern terrorists on the Internet as identified by Weimann, the researcher of the terrorist organizations' communications, as well as for psychological warfare; Advertising and propaganda; Data mining; Fundraising; Recruitment and mobilization of activists; Networking; Exchange of information; Planning and coordination.[44] However, despite the heavy presence in the cyberspace, it appears that neither the IS organization nor its supporters online, have the ability to execute significant cyber-attacks.

THE ISLAMIC STATE ON THE INTERNET

The IS organization has a prominent presence on the Internet and it is primarily of the first type of cyber activities, as defined above – that is, "use". The presence extends across many platforms, both dedicated websites such as Halummu and Shamukh, as well as the social networks and instant messaging services built around them, such as Twitter, Facebook and Telegram, with central and official origins, supporters and even bots working to streamline the distribution process. Thus, while media advocacy and dissemination groups online have official status and are subject to the organization's media laws, the IS organization has never officially recognized a pro-IS cyber group. This has led to the creation of a diverse collective of support groups working unofficially for the organization and identified with the organization by name and logo alone.[45]

OFFENSIVE CAPABILITIES

Hackers who identify themselves with the activities of the IS organization have in recent years carried out cyber activities that do not amount to a physical cyber threat or actual damage. These actions included, as detailed in the comprehensive review above, mainly hacking and defacing various sites around the world, as well as hacking into user accounts on the social media networks where content was published supporting the organization. In addition, hackers leaked personal

[43] Conway, M. (2002). Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet. Dept. of Political Science, Trinity College, Dublin Ireland. *First Monday*.
[44] Weimann, G. (2004). How Modern Terrorism Uses the Internet, *United States Institute of Peace, Special Report*. No. 116.
[45] Bernard, R. (2017) These are not the terrorist groups you're looking for: an assessment of the cyber capabilities of Islamic State, *Journal of Cyber Policy*, 2:2, 255-265.

information, mainly from databases of organizations and entities in the United States.[46] It seems that the heavy presence online, supported by the mirror created by the media around it, has led to the widespread – and misleading – perception that the IS has high cyber capabilities not only with respect to the ability to generate and disseminate propaganda, but also with regard to the ability to launch cyber-attacks. In reality, a comprehensive review of the IS organization and its support groups throughout the internet shows that they have not demonstrated the cyber capabilities required to carry out significant offensive campaigns, and that the focus on choosing the targets for the attack remains attacks against physical targets in the traditional way.[47]

Having said that, in May 2017 WannaCry attack took place, the largest cyber-attack in history. The attack also provoked reactions among IS supporters on the internet, followed by a publication by the Fighter Moeslim Cyber Caliphate on its Telegram channel of a screen shot documenting a cyber-attack it had carried out – an imitation of the WannaCry ransomware. The hacker FMCC, identified with vandalism type cyber-attacks and the use of ransomware is unusual due to the nature of the attack aimed at achieving economic gain. Moreover, the move reflects an aspiration to create similar attack tools and a thought process geared at developing and refining offensive capabilities.[48]

DEFENSIVE CAPABILITIES

A technical means often used by the IS organizations as a means of securing information is a checksum, for the protection of the integrity of information. This code is mainly used by channels that produce official IS media content such as the Telegram channel, Khilafa News, which is a secondary source for the publication of IS news or the Amaq app, a news agency affiliated with the organization.[49]

Left: A screenshot from the KhilafaNews Telegram channel ; Right: banner of the Amaq app

[46] Pavel, T. (2017). Physical Threats in Online Worlds — Technology, Internet and Cyber under Terror Organization Services; a Test Case of the Islamic State", *International Journal of Information Security and Cybercrime 6.* Available online at: http://www.ijisc.com/articles/2017-01-09.pdf

[47] Bernard, R. (2017) These are not the terrorist groups you're looking for: an assessment of the cyber capabilities of Islamic State, *Journal of Cyber Policy*, 2:2, 255-265.

[48] Cyber Desk c, (01.06.2017). Cyber review no. 22 *International Institute for Counter Terrorism (ICT)*. https://www.ict.org.il/Article/2098/cyber-review-no-22#gsc.tab=0

[49] Ibid

Additional defensive technical measures can be found in the publications of the Electronic Horizons Foundation group, the only official cyber group operating on behalf of the IS. It operates groups, telegram channels and group chat rooms on the Riot app, and duplicates backup channels for cases where its channels of activity are closed by the enabling platform. Electronic Horizons Foundation serves as a kind of "technical support" (Help Desk) for the Muslim community online and its operators regularly publish recommendations for safe use of the network, accompanied by illustrated digital guides that help users download and install recommended software; The group's operators also advertise tips for protection of privacy; Answering questions from surfers; A review of previous recommendations and their update. The uniqueness of the group is in making the technological content accessible to a popular audience alongside simplification and explanations for laymen. Thus, the core of the activity on the defensive side is not the development of technological means, but rather the education of the Muslim community for safe use of the Internet.[50]

4. Discussion and Conclusions

It appears that the widespread use on the part of pro-IS cyber-terrorists in cyberspace remains "use" for terrorist purposes and does not amount to cyber-attacks. An examination of the technical aspects shows that the organization's defense system is comprehensive and well-established compared with the offensive system, reflecting the organizational needs that justify investment of resources in defense infrastructures rather than on attack. At the same time, it appears that the organization's supporters on the internet, as seen in the test case of the Fighter Moeslim Cyber Caliphate, do strive to develop and improve offensive capabilities; It is not possible to exclude the possibility that if independent development of offensive capabilities was unsuccessful – these can be purchased on the network, and therefore consideration must be given not only to ability but also to desire.

It is not inconceivable that the poor ability shown by the groups identified with the organization is a hurdle that has not yet been overcome and because of which there is no official recognition of them by the IS. It is similar to claiming responsibility for a terrorist attack in the physical world. On this manner, the organization does not claim responsibility for negligible attacks in terms of the impact on the public, since it must maintain a standard and present a strong and threatening appearance. Any claiming of responsibility for a minor event is liable to harm the organization's reputation in the eyes of its supporters. Similarly, in cyber-attacks – until a successful cyber-attack is launched –

[50] Cyber Desk a, (01.05.2017). Cyber review no. 21. *International Institute for Counter Terrorism (ICT)*. https://www.ict.org.il/Article/2097/cyber-review-no-21#gsc.tab=0

the organization will not take responsibility for failed attempts by its supporters, and it may be a matter of time before a successful cyber-attack will justify official claiming of responsibility.

Virtual defacement is a *computer* crime and its physical counterpart (graffiti) is an offence against *property*. Murder, on the other hand, is a *violent crime* and an offence against the *person*. These are completely different offenses, each of which is based on a different criminal intent.

The assumption that the UCC did – and still may – have plans to carry out a cyber-attack that would pose a significant security threat could explain the elimination of the UCC leaders by the Americans. The UCC had three leaders and the three were eliminated by American drone attacks: Junaid Hussain, Siful Haque Sujan and Osed Agha. The possibility that the Americans have invested military resources in these eliminations for defacement attacks, denial of service (DDoS) and leakage is unlikely. And therefore, in this sense the elimination of the three can be attributed to an operational need to prevent attacks. But since their activities are not dedicated to cyber-attacks and information security activities, we believe that *the UCC leaders have been eliminated because of the entirety of the activities* they have carried out for the IS, which include hacking, information security, propaganda and recruitment online; And not because of their technological capabilities in themselves. This assessment is in line with the elimination of Sally Jones due to her online activity, which included recruitment and propaganda on behalf of IS but not hacking or information security.

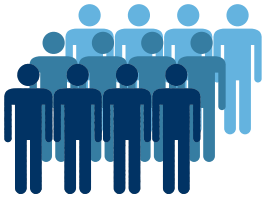
It is interesting to note that the UCC leaders were all of South Asian origin to a certain extent. Junaid Hussain was of British-Pakistani origin. His successor, Siful Haque Sujan, was of Bengali origin. And Osed Agha was, according unverified reports on social networks, of Indonesian origin. This is a trend of shifting from a focus in the United States and Western countries towards focusing on Southeast Asia. Other expressions of the trend are documented in UCC publications encouraging

cyber-attacks in Southeast Asia and summarizing the results of cyber-attack campaigns that indicate *an increase in the scope of activity of pro-IS activists in Southeast Asia*. Another expression is a language analysis, which shows that while in the past the communication between the UCC activists was in English and Arabic, now it is almost entirely in Indonesian.[51]

The hacktivism activities of IS-supporters have intrinsic value because they generate the media noise that terrorism is aiming for in the first place.

This position is supported by the fact that the level of cyber-attacks by IS-supporters online has remained low in recent years,

while the scope of the groups has increased exponentially.



This being said, an estimate from another angle must also be taken into account. The review shows that, with the exception of specific incidents, most of the hacking activities of the pro-IS supporters are activist (protesting), low-level, and – apparently – carried out by teenagers.[52] The hacktivism carried out in support of the IS is a unique feature of the *cyberculture* of the jihadist community on the Internet, in which the *Muslim-virtual public sphere* is realized. In this sense, there is a vast difference between a virtual protesting act of teenagers and the planning and execution of a multi-casualty attack with kinetic consequences in the physical world. Not everyone who makes virtual protest will necessarily kill using cyber tools, just as not everyone who paints graffiti on the property of others will necessarily kill using a weapon.[53] On the contrary, the relative ease with which it is possible to carry out activist hacking versus vandalism in the real world increases the distance between these offenses and the crimes causing death. Thus, it can be argued that those who choose to carry out hacktivist cyber-attacks are probably young people who lack the psychological

[51] For further details, see the ICT report from December 2018 titled, "Islamic State-Supporting Hacktivists in Southeast Asia" at: https://www.ict.org.il/Article/2308/isis-hacktivists-south-east-asia-hebrew#gsc.tab=0
[52] https://www.bleepingcomputer.com/news/security/interpol-and-security-firm-dox-pro-isis-hacktivists/ accessed January 19, 2019
[53] It is common to compare the offenses of Web site defacement and graffiti in the virtual world

capacity to deal with the dangers and consequences of action in the physical world. They operate in cyberspace *because* this space allows ease of operation and low risk of being apprehended; Otherwise they would not have been able to participate in the protest. A virtual offense of protest (mainly defacement) is a *computer* crime and its physical counterpart is an offence against *property*. Murder, on the other hand, is a *violent* crime and an offence against the *person*. These are completely different offenses, and each of them has a different criminal intent. Moreover, the hacktivism activities of IS-supporters have intrinsic value because they generate the media noise that terrorism is aiming for in the first place. This position is supported by the fact that the level of cyber-attacks by IS-supporters online has remained low in recent years, *while the scope of the groups has increased exponentially*.

Hacktivism offenses are minor offenses and do not pose a *direct* threat to security. However, the necessity of dealing with them should not be taken lightly. Criminology has a theory called "*broken windows*" whereby when there is a broken window in a building that is not repaired, soon all other windows will be broken, the door will be taken out and the place will become a drug den. A broken window symbolizes neglect that "invites" a similar treatment that in turn leads to deterioration.[54] The key to preventing crime is, in the authors' opinion, in locating and repairing the "broken windows" immediately so as to *prevent the deterioration continuum*. This theory was what former mayor of New York (and currently advisor to US President Trump in the field of cyber protection), Rudy Giuliani, relied on in the eradication of crime; He focused on thwarting minor offenses and a policy of "zero tolerance" toward small details. Giuliani issued a directive forbidding subway cars to leave the station if graffiti was painted on them, until the graffiti was removed from them. It turned out that graffiti artists were looking for an audience for their works and once the cars had been cleaned without anyone seeing their work – their motivation was gone and they stopped drawing graffiti on subway cars. In Giuliani's tenure, the overall crime rate dropped by 57 percent, murders dropped by 65 percent, and the FBI recognized New York as the safest large city in the United States. it is possible that adopting a similar policy may also be helpful here.

[54] Wilson, James Q; Kelling, George L (Mar 1982), "Broken Windows: The police and neighborhood safety", *The Atlantic.* Manhattan institute). Available online https://www.manhattan-institute.org/pdf/_atlantic_monthly-broken_windows.pdf. accessed January 16, 2019.