IDC HERZLIYA | ICT International Institute for Counter-Terrorism
With the Support of Keren Daniel

ICT Cyber-Desk

PERIODIC REVIEW

Cyber-Terrorism Activities

Report No. 18

July - September 2016

Contents

Highlights

This report covers the period of July-September 2016, on 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 following are the main issues covered in this report:

- Terrorist organizations continued to carry out propaganda activities and to disseminate messages aimed at supporters and potential recruits. The Islamic State focused on encouraging individual terrorist attacks in countries battling terrorism using the element of imitation – glorifying previous successful attacks, such as the attack in Nice, France. Al-Qaeda continued its efforts to expand the channels through which it distributes its messages, with emphasis on the Indian Subcontinent. It can be assumed that these efforts stemmed from, among other things, the growing competition between Al-Qaeda and the IS, which is losing strongholds in the battle arena in Syria and Iraq, and is therefore establishing main centers in other areas.
- During the period under review, jihadist organizations in the Gaza Strip identified with the IS and Al-Qaeda focused on the Internet as a source of fundraising, while other organizations continued their fundraising efforts through more traditional channels.
- Terrorist organizations were aware of preventative efforts by security agencies and major players on the Internet in general, and on social networks in particular, to remove jihadist content from their platforms. In response, these organizations continued to distribute defensive guidelines and instructions, and to expand their activities on the darknet where they claimed to be better able to protect traffic and anonymity.
- Terrorist organizations continued their efforts to improve their offensive capabilities, but at this stage they did not reveal significant technological abilities in this area. Nevertheless, it should be taken into account that these organizations can hire external bodies, such as those who identify with terrorist ideas or organized crime, and can acquire such abilities from terrorism-supporting states.
- During the month of July 2016, the GhostSquadeHackers group launched an offensive campaign titled, “OpReverseCaliphate” against IS-supporting hackers. The attack mainly

targeted the United Cyber Caliphate group, which is identified with the IS and composed of several hacker groups.

Introduction

In recent years, cyberspace has become a combat zone as well as an important and integral part of the current and future battlefield. In this framework, cyberattacks have been on the rise against state targets, critical infrastructure and business sites by countries (that do not claim responsibility), hacker groups (such as Anonymous), organized crime and individual hackers. These activities, which garner extensive international coverage, have led many countries to develop safeguards, as well as offensive capabilities, as part of their national security programs.

Terrorist organizations, which are also operating in this changing and dynamic environment, are strengthening their hold on cyberspace, which they refer to as "electronic jihad",[1] especially global terrorist organizations. However, such activity goes beyond the classic recipe of Internet use as a means of contact, recruitment, financing, publicity, incitement, psychological warfare and intelligence. Jihadist organizations are working on developing offensive capabilities in cyberspace, integrating the virtual world and the real world.

The following document is a periodic report based on information that was collected and analyzed by the CYBER DESK, distributed as part of the worldview of the International Institution for Counter-Terrorism (ICT) according to which "sharing knowledge is a force multiplier in combatting terrorism". The document covers two main subjects: CYBER TERRORISM (offensive, defensive, and the media, and the main topics of jihadist discourse) and CYBER CRIME that is linked to the jihadist organization activity (funding, methods of attack).

[1] https://www.ict.org.il/UserFiles/JWMG_Electronic_Jihad.pdf

Operational Usage by Jihadist Organizations

Terrorist organizations continue to use the Internet for a wide range of uses, including a continued process of professionalization and emphasis on various social networks as a platform for distributing messages and guidance to various sites.

Jihadist Propaganda

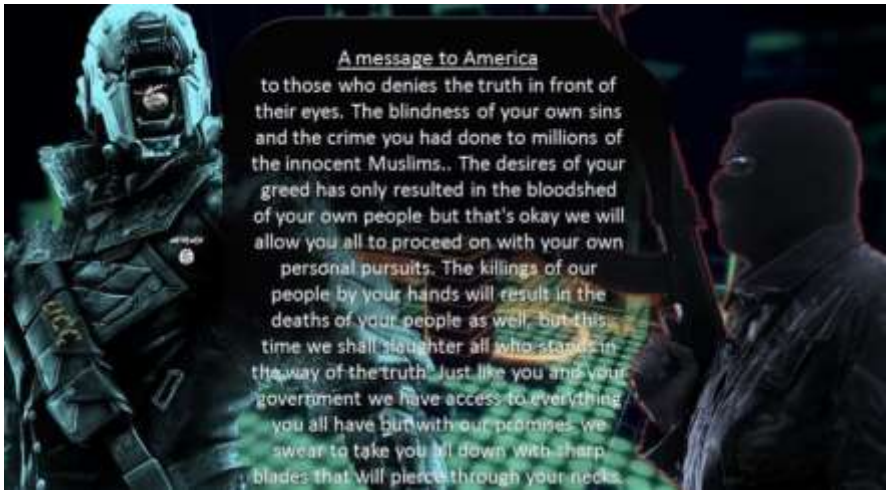
During the period under review, jihadist organizations continued to carry out propaganda activities with familiar features to the past.

The IS continued to carry out propaganda activities and to disseminate messages aimed at supporters and potential recruits. This activity intensified as the organization continued to lose battles in Syria and Iraq, territories and the sources of funding that come along with them, and the halo adorning its supposed victories on the battlefield. In an effort to draw the public's attention away from these losses, beyond its efforts to blur and distort reality, the organization encouraged individual terrorist attacks in countries battling terrorism using the element of imitation – glorifying previous successful attacks, such as the attack in Nice, France. Al-Qaeda continued its efforts to expand the channels through which it distributes its messages, with emphasis on the Indian Subcontinent. It can be assumed that these efforts stem from, among other things, the growing competition between Al-Qaeda and the IS, against the backdrop of the general assessment that the IS will shift its center of gravity from the battlefields in Syria and Iraq, where it is waging a battle of survival, to regions with a low degree of governability.

Among the activities worth noting:

Propaganda related to the Islamic State

- The United Cyber Caliphate, which is identified with the IS and is part of the Islamic State Hacking Division, distributed several posters threatening the US and Egypt during the month of July 2016.



Screenshots from Telegram

- Al-Nusra Al-Maqdisiyya jihadist media group, which mainly covers Palestinian jihadists inside the Gaza Strip and beyond (such as the Sinai Peninsula), launched a Telegram

channel on July 13, 2016 to help spread propaganda for the IS.[2] Among other things, this channel publishes messages of encouragement for lone wolf attacks, such as the ramming attack in Nice, France.

The banner of the Telegram channel of "Al-Nusra Al-Maqdisiyya"

The last will and testament of the terrorist who carried out the ramming attack in Nice as it appeared on the Telegram channel of "Al-Nusra Al-Maqdisiyya"[3]

- United Cyber Caliphate, which is identified with the IS, called on lone wolves to carry out terrorist attacks through a poster on Telegram that was published on July 19, 2016. The poster suggested various methods of attack: shooting, stabbing, blowing up, ramming, stone throwing, poisoning, hitting and screaming [sic]. The poster included two quotes

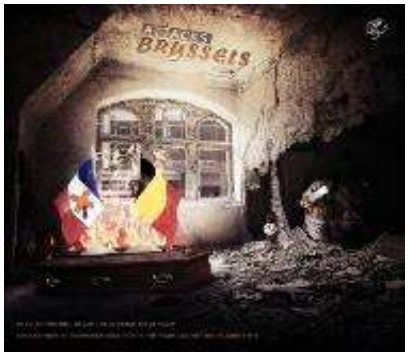
[2] 13.7.16. Telegram channel.
[3] 26.7.16. Telegram channel.

from the Quran justifying attacks against anyone who does not believe in the Quran.

A screenshot of the poster on the Telegram channel of the United Cyber Caliphate

- During the months of July-August 2016, the Bushriyyat al-Wa'y media group, which supports the IS, published on its Telegram channel threats to attack American targets on Turkish soil and to continue the wave of attacks against France, mentioning the ramming attack in Nice and posting photos showing the Eiffel Tower in flames.[4]

[4] July-August. Telegram channel



Threats to attack France

Threats by the IS to attack the US Air Force at Incirlik Air Base in Turkey

- During the first half of August 2016, IS supporters published on a variety of Telegram channels calls on Muslims living in the West to act for the release of Muslim prisoners

sitting in jails in the West.[5]

The banner subtitles: "Let us Destroy the Prisons"

- In August 2016, Al-Sumud jihadist media institution, which supports the IS, published on its Telegram channel links to download two anthologies containing a collection of the organization's publications in Somalia and the Maghreb.[6]

From left to right: a collection of publications by the IS in the Islamic Maghreb; the IS in Somalia

- The following are some of the publications on the Bank al-Ansar Telegram account of the Afaq group, which is involved in IS publications regarding cyber issues (the Telegram account was opened on March 8, 2016):
    - An appeal to followers of the group's Telegram channel to help distribute the mujahideen's official propaganda materials that were removed from social

[5] 16-26.8.16. Telegram channels
[6] 12.8.16. Telegram channel

networks, especially Twitter and Facebook.[7]

- A graph detailing the channel's PR activities during the period between March 8, 2016 and June 8, 2016, according to which 5,900 Twitter accounts and 600 Facebook accounts were activated by 6,500 supporters of the organization (see photo).[8]

- A graph detailing the channel's PR activities during the month of July 2016, according to which 2,429 Twitter accounts and 358 Facebook accounts were activated by 2,787 supporters of the organization (see photo).[9]

[7] 9.3.16. Telegram channel.
[8] 20.7.16. Telegram channel.
[9] 20.7.16. Telegram channel.

- A graph detailing the channel's PR activities during the month of August 2016, according to which 2,489 Twitter accounts and 568 Facebook accounts were activated by 3,057 supporters of the organization (see photo).[10]

- The Islamic State's publishing house, Al-Himmah Library, published a second version of the "Learning Letters" application designed to teach children the alphabet and numbers in Arabic on Android computers and devices.[11]

[10] 20.7.16. Telegram channel.
[11] 23.9.16. http://addpost.it/2443; https://dawaalhaq.com/post/53344

Banners publicizing the second version of the "Learning Letters" application

- On July 28, 2016 the Yaqeen Media Foundation, which is involved in publicity for the IS, published a graph detailing the hacking attacks (details of the attacks appear under the "Offensive Tactics" chapter of this report) that were carried out by the United Cyber Caliphate group, which is identified with the IS.

Propaganda related to Al-Qaeda

- Al-Sahab jihadist media institution, which belongs to Al-Qaeda, launched its official Telegram channel on July 3, 2016.[12]

The logo of Al-Sahab

- *Al-Masra* magazine, which belongs to Al-Qaeda in the Arabian Peninsula (AQAP), published issue no. 20 on August 26, 2016, in which it announced that the Telegram channel "News of the Nation" will be the magazine's exclusive publisher. [13]

The announcement regarding the publication of *Al-Masra* content on the "News of the Nation" Telegram channel

- The Usama Media jihadist media institution, which serves as a platform for the publications of Al-Qaeda in the Indian Subcontinent in the Bengali language, launched a Facebook page, Twitter account and blog in the beginning of August 2016. [14]

[12] https://telegram.me/sahabof2 ; https://twitter.com/As_Sahab_/status/766549049369436160
[13] http://up.top4top.net/downloadf-238i03r0-pdf.html
[14] https://www.facebook.com/USAMAMEDIA/; https://twitter.com/usama_media; https://usamamediaweb.wordpress.com/home/.

The Facebook page of Usama Media

- The Global Islamic Media Front (GIMF) jihadist media institution, which serves as a platform for the official publications of Al-Qaeda in the Indian Subcontinent, launched a Telegram channel on August 1, 2016.[15]

The announcement regarding the launch of the GIMF Telegram channel

Radicalization

During the period under review, radicalization activities continued to be carried out on the Internet (in addition to similar activities in the physical world), as part of the overall trend of the growing use of the cyber world. In this manner, terrorist organizations and the parties associated with them make use of platforms with broad distribution but, at the same time, hide their identities and traffic as much as possible.

In the framework of this report, we chose to mention several incidents in which young people underwent a process of radicalization that ended in their decision to act in the name

[15] Telegram channel.

of the Islamic State:

- In August 2016, information was received concerning a 23-year-old Canadian man named Aaron Driver from Ontario, Strathroy, who had tried to carry out a suicide attack,[16] following his involvement in the Islamic State's social media community. According to this information, Driver was radicalized via social networks (at least Facebook and Twitter), after making online contact with IS supporters, where he openly expressed full support for the organization's activities. Driver managed several profiles under various identities, including one a Twitter account under the name 'Haroon Abduraham'. The profile on this Twitter account was supported and promoted by a community of IS supporters on the Internet. Driver expressed concerns regarding the monitoring and arrest of IS activists and supporters, and he even noted that he had taken the necessary precautions to maintain safety on the Internet, including using the Tails operating system, which enables anonymous and secure surfing and transmission of instant messages.[17] Driver was killed in an operation by Canadian police forces in southern Ontario, Canada, after he was suspected of planning a suicide attack in one of the largest cities in Canada [18] and was even identified by the Islamic State's *Amaq* news agency as an IS soldier.

A photo of Aaron Driver

- Ahmad Khan Rahami was a young man of Afghan origin who planted bombs in New York

[16] https://www.rt.com/news/355477-canada-suicide-bomber-suspect-police/
[17] http://www.cbc.ca/news/canada/manitoba/aaron-driver-peace-bond-terrorist-isis-1.3430287
[18] http://www.ctvnews.ca/politics/lone-suspect-killed-in-anti-terrorism-operation-in-southern-ontario-1.3023694?hootPostID=b57f369aef74ce39835920bc3a0e08df

and New Jersey in September 2016.[19] Rahami's radicalization process apparently began during his visits to Afghanistan and Pakistan, and continued via social networks.[20] Since 2010, he was active on several social networks simultaneously, including YouTube, Twitter, AOL, Lifestream and tagged. These accounts included general information about his studies, work, etc., with no indication of his outright support or activities for the IS. Nevertheless, notebooks were found in Rahami's belongings that contained personal records in which he referred to speeches by al-Adnani that were published on social networks, as well as IS propaganda materials. In addition, information was found indicating that Rahami had done a search on e-Bay to purchase raw materials that could be used to assemble an explosive device. This does not rule out the possibility that reason evidence of Rahami's support for terrorist activity was not found was because he deleted it as part of the cyber-defense actions taken by terrorists and terrorism supporters, and in light of the widespread distribution of jihadist guidebooks on this issue. It should be noted that Rahami's father, Mohammad Rahami, and his sister, Aziza Rahami, were active on social networks and distributed jihadist content to their friends,[2221] accounts that were closed for this reason on September 20 and 21. Aziza's account also included sermons by the Islamic preacher, Khalid Yasin, and tweets by IS fighter, Farah Mohamed Shirdon. [23]

[19] https://www.theguardian.com/us-news/2016/nov/16/ahmad-khan-rahami-indicted-new-york-new-jersey-bombings

[20] http://www.nj.com/union/index.ssf/2016/09/7_things_to_know_about_charges_against_ahmad_khan_rahami.html ; http://edition.cnn.com/2016/09/19/us/ny-nj-bombings-rahami-afghanistan-trips/index.html ; https://news.vice.com/article/ahmad-khan-rahami-bought-his-bomb-parts-on-ebay-fbi-says

[21] http://www.dailymail.co.uk/news/article-3798726/Pictured-Pakistan-trip-changed-tubby-terrorist-brother-posted-pro-jihad-messages-online.html

[22] http://pamelageller.com/2016/09/more-evidence-of-ny-bombers-familys-jihad.html/

[23] http://www.telegraph.co.uk/news/2016/09/21/ahmad-rahamis-sister-posted-radical-material-online-as-police-qu/

The FBI poster with details about Ahman Khan Rahami

Terror Fundraising

During the period under review, jihadist organizations in the Gaza Strip that identify with the IS and Al-Qaeda focused on the Internet as a source of fundraising. It is worth mentioning the growing fundraising difficulties facing the Islamic State, which is waging a campaign of survival in Syria and Iraq, and the depletion of its sources of funding despite being a hybrid organization, which to some extent affects the entities associated with it. Considering the current state of affairs, it can be assumed that fundraising attempts using Internet platforms will increase.

Ahfad al-Sahaba, a Palestinian Salafi-jihadist organization operating in the Gaza Strip and identified with the IS, launched its official Telegram channel on August 22, 2016. An online fundraising campaign called "Jahizuna" ("Equip Us") was publicized on the channel – a campaign that was started approximately two years ago and designed to equip the organization's fighters with weapons to "clash with the Jews" and to "free prisoners", according to its organizers.

It should be noted that this campaign competes with another fundraising campaign called

"Jahiz Ghaziyan" (Equip a Warrior"), which is run by Jaysh al-Umma al-Salafi, another Salafi-jihadist organization operating in the Gaza Strip but identified with Al-Qaeda. Among the goals of this campaign, as noted on the organization's Twitter account: implementing the idea of the Oneness of God among the population, helping the poor, liberating Islamic holy places and supporting Muslims who act to spread the idea of the Oneness of God in Palestine, helping with propaganda against deviant Muslim groups such as Shi'ites, helping orphans whose parents died as martyrs, and helping prisoners and the wounded.

From left to right: the banner that was produced in the framework of the "Equip Us" fundraising campaign; the logo of the Telegram channel of Ahfad al-Sahaba, a supporter of the IS

From left to right: the banner of the "Equip a Warrior" campaign by Jaysh al-Umma al-Salafi, a supporter of Al-Qaeda; the list of weapons that the organization seeks to purchase thanks to the fundraising campaign

Cyber Defensive Tactics

Terrorist organizations are aware of the tireless preventative efforts of security agencies and major players on the Internet in general, and on social networks in particular, to remove jihadist content from their platforms. Therefore, these organizations continue to distribute defensive guidelines and instructions, and to expand their activities on the darknet where they claim to be better able to protect the traffic and anonymity of the organizations themselves, as well as their supporters, from the tracking software of intelligence agencies and activists who operate against terrorist organization on the Internet.

Organizational support for cyber-defense continued with the translation of guidebooks produced by elements unconnected to terrorism, and with the independent production of guidebooks, instructions and warnings about malware.

Defense Activities

- One of the administrators of Al-Fida jihadist Web forum, which supports Al-Qaeda and its branches, known as Abu Jihad al-Muhandis, recommended that forum users use TOR software.[24]

A screenshot from Al-Fida jihadist Web forum

- Amaq news agency, which belongs to the IS, continued to publish Mozilla's plug-in for

[24] 30.9.16. http://alfidaaforum.net/vb/showthread.php?t=116665

Firefox, which is designed to make it easier for users to access reports and publications related to the IS that were removed and re-published on a different Web site.[25] According to Google data, approximately 7,200 Web surfers used the plug-in during the month of August 2016, of which approximately 1,400 were from Turkey, approximately 600 from Saudi Arabia, approximately 500 from Egypt, approximately 400 from the United States, approximately 200 from Algeria and approximately 70 from Germany. It should be noted that a similar guidebook for using this plug-in was published in the past.[26]

The banner that was distributed, including guidelines for installing the plug-in for Firefox browser

- Amaq news agency, which belongs to the IS, released the third update of its application, "Amaq", which serves to distribute news about the organization to the public browsing on mobile phones based on the Android operating system. [27]

[25] Telegram channel.
[26] For further reading, see Cyber Report no. 16: https://www.ict.org.il/UserFiles/ICT-Cyber-Review-16.pdf
[27] 15.8.16 . Telegram channel.

The banner announcing an update for the "Amaq" application

Defense Guidebooks

- The Afaq group is involved in publicity for the IS and publishes news regarding the cyber world. The following are some of the publications that appeared on the organization's Telegram channel during the period under review:
    - A link to a guidebook on installing and using Threema, an off-the-shelf software used for encrypted chat, which was first released in March 2016.[28]

The banner that appeared on Telegram

    - Links to a series of guidebooks titled, "Computer Security Course", which cover – among other things – virus security; installation and use of Windows, Mac and Linux and Unix operating systems; protection against Keylogger; file encryption using the Vera Crypt software for Windows; USB encryption and file deletion;

[28] .6.3.16 https://justpaste.it/threema1

protection of Twitter accounts from breaches; VPN and other services.[29]

The banner of the computer security course

A guidebook on how to protect a Twitter account from being breached

- A video of a course on the secure use of mobile phones.[30]
- A guidebook on how to open a fake Twitter account using the VPN and Hide.me applications and the Firefox browser on Android phones and iPhones. [31]

[29] 26.7.16. https://justpaste.it/twsec;
[30] 29.7.16. Telegram channel; https://drive.google.com/file/d/0B0QtafudKnayeU5rcUxZZ29HdU0/view
[31] 26.8.16. Telegram channel.

The banner that appeared on Telegram

- Links to a series of articles titled, "About Security", which dealt with protecting Twitter accounts from hacking; coping with attempts by the Twitter administration to remove the accounts of mujahideen; safe conduct when using Twitter; hostile spying software (spyware) on social networks; raising awareness about the dangers of exposure to intelligence gathering about users when using the Google search engine.
- A link to a guidebook regarding the careful and secure use of smartphones.

- Issue no. 10 of the *Dar-al-Islam* magazine, which is published in French by the IS, included a guidebook on the secure use of mobile phones (pp. 38-46). For instance, the guidebook advised installing VPN or TOR software on mobile phones, and using encrypted chat software to send messages.[32]

[32] 20.8.16. https://archive.org/details/DrAlIsllm10

Pages 38 and 42 of *Dar al-Islam* magazine

- During the period under review, various publications were posted on the Justpaste.it Web site, a platform that also serves jihadist elements, under the name Islamic Cyber Army, which is composed of IS-supporting groups and individuals primarily active in the field of cyber-attacks. On July 16, 2016 a guidebook was published on the site that explained how governments listen in on mobile phones. It should be noted that the article had already been published in May 2016 on an Arabic blog about information security called iSECUR1TY.

Offensive Tactics

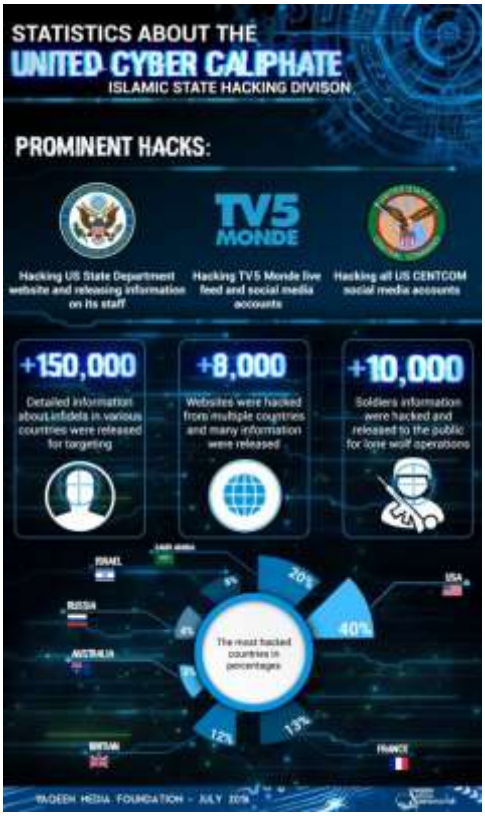
Terrorist organizations continued their efforts to improve their offensive capabilities, but at this stage they do not reveal significant technological abilities in this area. Nevertheless, it should be taken into account that these organizations can hire external bodies, such as those who identify with terrorist ideas or organized crime, and can acquire such abilities from terror-supporting states.

- On July 28, 2016 the Yaqeen Media Foundation, which is involved in publicity for the IS, published a graph detailing the hacking attacks that were carried out by the United Cyber Caliphate group, which is identified with the IS.

  A summary of the group's operations indicate the following points:

  - Over 150,000 personal details of people around the world were exposed.
  - Over 8,000 Web sites were breached and the details of over 10,000 soldiers defined as a target for attack by lone wolves were exposed.
  - The main targets of attack were the US (40%), Saudi Arabia (20%), France (13%) and Britain (12%).

The following graph notes that the group's successful cyber-attacks included the breach of the US State Department and the release of information about its staff, and the breach of French TV5 Monde's live feed as well as the station's social media accounts. In addition, it was claimed that all of US CENTCOM's social media accounts were hacked.



The banner of Yaqeen Media Foundation, which detailed cyber-attacks by the IS

- A member of Al-Minbar jihadist Web forum, which is identified with the IS, known as Ayyam Fath Baghdad, published a detailed electronic guidebook on tools for hacking Web sites. According to him, the guidebook was designed to help breach secure sites in the US and Europe, and to help establish a "group of electronic soldiers". The recommended hacking tools were based on Kali Linux. Visitors to the forum reacted sympathetically and expressed their desire to study the topic and become hackers for the IS.[33]
- On July 4, 2016 the Islamic Cyber Army group (a body composed of IS-supporting groups and individuals primarily active in the field of cyber-attacks) published on the Justpaste.it Web site (a platform that also serves jihadist elements) information about a breach of Saudi government databases and the lists that were stolen from them. The publication

[33] 21.8.16. http://www.almodon.com/media/2016/8/21/داعش-يسعى-لإنشاء-تنظيم-القراصنة ; https://www.mnbr.info/vb/index.php

contained screenshots of lists including employee details and financial data, but the quality was illegible and did not allow for validation of the data. In addition, lists were also published that contained names and personal email addresses. An examination of the data revealed that this list was taken from an Excel file on the Web site of King Faisal University and included details about students who did their internships in government offices.

Cyber-Crime and Cyber-Terrorism

Recent years have seen an increasing number of cyber-attacks against political targets, critical infrastructure, and the Web sites of commercial corporations. These attacks, which receive increasing amounts of international attention, are perpetrated by states (which do not claim responsibility for them), groups of hackers (such as Anonymous), organized crime and lone hackers. We believe that terrorist organizations are working in close collaboration with organized crime to learn from their attempts [at cyber-crime] and may even be hiring their services. In light of this, it is important to examine and analyze cyber-crimes attributed to criminal organizations, as well as new development trends and patterns.

The following information was culled from the visible (OSINT) and invisible ("Dark Web")[34] Internet between July - September 2016.

Cyber Terror and Cybercrime Counter Measures

- In the beginning of July 2016, the European Commission decided to establish a public-private partnership for investment in the field of cyber-security. In the framework of the partnership, the EU would invest 450 million Euros as part of the multi-year investment in research and development of the Union – Horizon 2020. It is estimated that, as a result of the new program, approximately 1.8 billion Euros will be invested in the European market by various sectors by 2020, which will improve Europe's ability to cope with cyber-attacks.[35]
- The risk analysis that was performed by Europol at the end of September 2016 indicates the possibility of a future connection between cyber-crime and terrorist organizations seeking to attack EU countries. The report further states that terrorist organizations are working to create a threatening image as part of their psychological warfare efforts, but in practice most of the attacks are carried out through security breaches and known

[34] The "dark Web" or darknet is "A collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks." See P. Biddle, P. England, M. Peinado and B. Willman (no date), "The Darknet and the Future of Content Distribution", *Microsoft Corporation*, http://msl1.mit.edu/ESD10/docs/darknet5.pdf.
[35] www.europa.eu/rapid/press-release_IP-16-2321_en.htm

hacking methods. [36]

- Europol conducted a 48-hour operation against online terrorist propaganda that was shared by radical groups and sympathizers, which was coordinated with International Referral Units[37] from France, Germany, UK and Slovenia. The operation included the processing of 1,677 social media accounts and content in six languages in order to contain terrorists and their violent and extremist propaganda. Europol released a statement explaining that it had found content that included online terrorist propaganda hosted by 35 social media and online service providers.[38]
- A senior executive at Google, Diane Greene, stated that the company informs approximately 4,000 Google users per month about attempts to attack their accounts by a state-sponsored body.[39] The company started sending such messages in 2012.[40] It can be assumed that the announcement refers to attempted breaches of email addresses. [41]

A screenshot including Google's warning of an attempted breach

- In August 2016, the Pakistani Parliament approved a change to the cyber-crime law that included more severe punishment for cyber-terrorism offenses, up to 14 years imprisonment and a fine of five million RS (approximately 75,000 dollars). [42]
- In early September 2016, a court for cyber affairs began to operate in Malaysia. The 27 judges who serve in the court underwent training on cyberspace in general and cyber

[36] https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime
[37] Internet Referral Unit
[38] https://www.europol.europa.eu/newsroom/news/counter-terrorism-specialists-team-to-take-down-online-terrorist-propaganda
[39] http://www.reuters.com/article/us-google-cyberattack-idUSKCN0ZR2IU
[40] https://security.googleblog.com/2012/06/security-warnings-for-suspected-state.html
[41] http://www.reuters.com/article/us-google-cyberattack-idUSKCN0ZR2IU
[42] http://www.dawn.com/news/1276662

forensics in particular.[43]

- Authorities in Kuwait arrested a civil servant named Othman Zebn Nayef for collaborating with the Cyber Caliphate Army (CCA).[44] Nayef is suspected of hacking the official Web sites of foreign countries and defacing them with the organization's ideology. The organization also stated that Nayef used his office computer to hack into social network accounts. It should be noted that Nayef's arrest provided information that led to the arrest of two more suspects from Iraq and Jordan.[45]

- An unknown party released an Android application that included Trojan horse software called SandroRat in order to collect information about US supporters. This application was distributed under the guise of an Al Bayan radio application.[46]

- Mohammed Shaheryar Alam, who was identified with "Cyber Sultan" who preached for the establishment of an Islamic state in Britain, was found guilty of promoting terrorism.[47] Alam is suspected of distributing terror-supporting content on the basis of information found on his laptop computer and cell phone. In addition, he shared links and videos, and was active in chat rooms.[48] As part of his activities, Alam asked visitors to watch IS videos,[49] promoted acts of violence, and celebrated on the anniversary of the 9/11 attacks in the US and the 7/07 attacks in London, England.[50]

[43] www.nst.com.my/news/2016/09/169883/malaysias-first-cyber-court-begins-operations-today
[44] http://www.reuters.com/article/us-kuwait-security-cyberarmy-idUSKCN1111CT
[45] http://24.ae/article/273866/%D8%A7%D9%84%D9%83%D9%88%D9%8A%D8%AA-%D8%A7%D9%84%D9%82%D8%A8%D8%B6-%D8%B9%D9%84%D9%89-%D9%85%D9%88%D8%A7%D8%B7%D9%86-%D9%8A%D9%86%D8%B4%D8%B1-%D8%A7%D9%84%D9%81%D9%83%D8%B1-%D8%A7%D9%84%D8%AF%D8%A7%D8%B9%D8%B4%D9%8A
[46] http://news.softpedia.com/news/isis-sympathizers-spied-on-using-trojanized-android-app-506661.shtml
[47] http://www.croydonguardian.co.uk/news/14586117.Thornton_Heath__Cyber_Sultan__convicted_of_spreading_Isis_propaganda_online/
[48] http://www.yourlocalguardian.co.uk/news/local/croydonnews/14591139._Cyber_Sultan__jailed_for_two_and_a_half_years_for_sharing_Isis_terrorism_video/
[49] http://www.croydonguardian.co.uk/news/14570893.Thornton_Heath_man__boasted_about_establishing_Islamic_State_in_the_UK___court_hears/
[50] http://www.thisislocallondon.co.uk/news/14591139._Cyber_Sultan__jailed_for_two_and_a_half_years_for_sharing_Isis_terrorism_video/

Significant Incidents

- In July 2016, a Ukrainian hacker breached the second largest telecommunications company in Poland, Netia,[51] and stole the company's customer database (updated as of 2014),[52] including personal details and business transactions.
- A report by Kaspersky Lab that reviewed cyber-attacks against major telecommunications companies revealed that, starting in 2015, there was an increase of about 45% in the extent and intensity of DDoS attacks (as compared to 2014), with the longest DDoS attack (over 12 days) having taken place in the second quarter of 2016. It also revealed an increase in the use of internal company parties by crime organizations, some voluntarily and some through the use of blackmail. [53]
- In July 2016, an information security analyst from Darktrace reported that at least four cyber-attacks had been carried out against the train system in Britain last year. According to the announcement, the attacks were designed to gather information and were believed to be carried out by a state or a state-sponsored group.[54]
- In the beginning of September 2016, Ben Gurion University published a study on the durability of US rescue forces' communications systems in the face of a TDoS attack. The study revealed that a successful attack is liable to paralyze the proper functioning of these systems and impair the ability of security forces to function.[55] It should be noted that TDoS attacks were used in the past as part of a combined attack, as a component designed to enhance the force of impact, such as the attack on the electrical system in the Ukraine in early 2016.

[51] www.reuters.com/article/us-poland-netia-cybercrime-idUSKCN0ZO22K
[52] https://www.hackread.com/ukranian-hacker-hacks-polish-telecom-netia/
[53] https://securelist.com/analysis/publications/75846/threat-intelligence-report-for-the-telecommunications-industry/
[54] www.telegraph.co.uk/technology/2016/07/12/uk-rail-network-hit-by-multiple-cyber-attacks-last-year/
[55] https://arxiv.org/ftp/arxiv/papers/1609/1609.02353.pdf

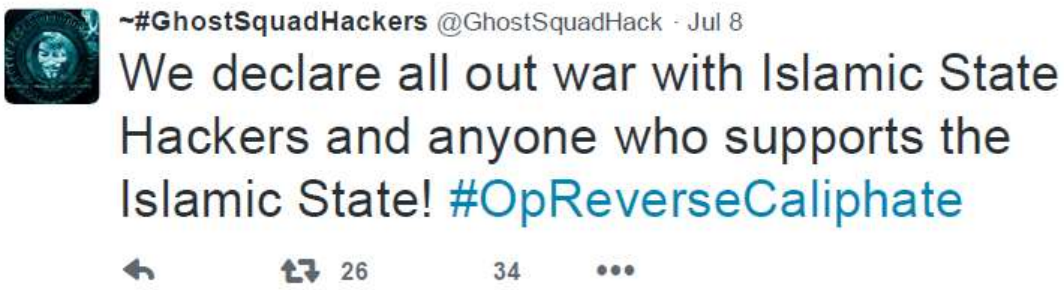
Case Study - GhostSquadeHackers vs. Islamic State

During the month of July 2016, the GhostSquadeHackers group launched an offensive campaign titled, "OpReverseCaliphate" against IS-supporting hackers.[56] The group includes activist hackers of various faiths, including Muslims, who are opposed to IS action and monitor the activities of over 10,000 IS supporters.[57] The attack mainly targeted the United Cyber Caliphate group, which is composed of several hacker groups including: Ghost Caliphate Section, Sons Caliphate Army, Caliphate Cyber Army, and Kalachnikov E-Security (Kakachnikiv.TN).

In the framework of the campaign, the identity of Moulaye Ahmed Ould Ahmed Semane of Nouakcho, who operates under the nickname "Mauritania Attacler", was revealed. According to the reports, this hacker acted together with AnonGhost, a pro-Palestinian and pro-IS hacker group operating primarily against Western countries.[58] The identity was also revealed of another hacker, Ouali Bouziad, one of the founders of AnonGhost and the United Cyber Caliphate (UCC) group. Another name that was exposed as a supporter of the organization was Harith al-Muhaji, aka Ansari Levantine or Romato.

It should be noted that about one month after the above-mentioned campaign, the GhostSquadeHackers group collaborated with AnonGhost to launch a cyber-attack against the State of Israel in response to an Israeli attack in the Gaza Strip.

The following are screenshots from the Twitter account of GhostSquadeHackers:



[56] http://anonhq.com/ghost-squad-doxs-members-united-cyber-caliphate-including-alleged-leader
[57] http://anonhq.com/ghost-squad-doxs-members-united-cyber-caliphate-including-alleged-leader
[58] See Cyber Report no. 17.

~#GhostSquadHackers @GhostSquadHack · Jul 8

Mauritania Attacker is the founder of United Cyber Caliphate and is the founder of AnonGhost he is one of the most skilled Isis hackers.

10 13 •••

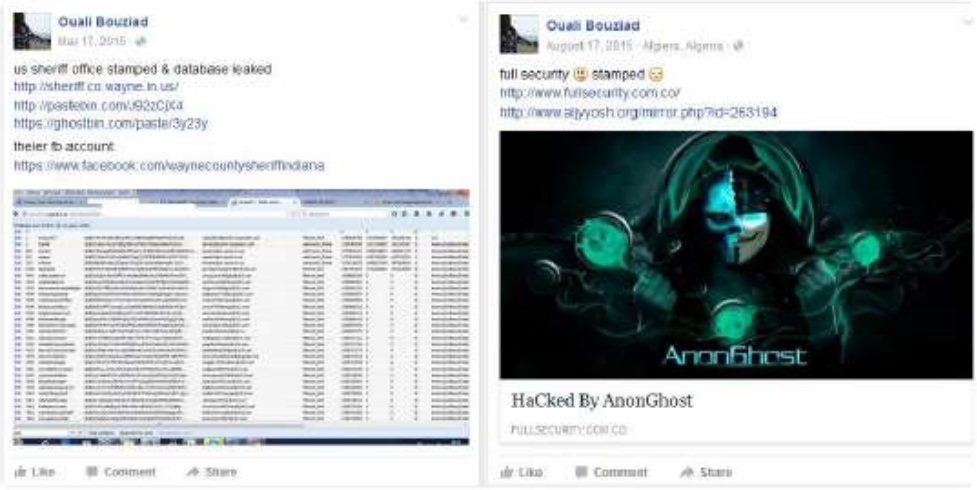
~#GhostSquadHackers @GhostSquadHack · Jul 9

AnonGhost Supports Isis this is no rumor, If you support AnonGhost than you support Isis its simple...

7 10 •••

~#GhostSquadHackers @GhostSquadHack · Jul 11

"Ouali Bouziad" Co-Founder of UCC and AnonGhost #OpReverseCaliphate
justpaste.it/w2e0
facebook.com/Extazy005



12 15 •••

Screenshots from Twitter

ICT Cyber-Desk Team

Dr. Eitan Azani, Deputy Executive Director, ICT

Dr. Michael Barak, Team Research Manager, ICT

Adv. Uri Ben Yaakov, Senior Researcher, ICT

Nir Tordjman, Cyber Desk Team Research Manager, ICT

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.

Click here for a list of online the ICT Cyber-Desk publications

For tailored research please contact us at Webmaster@ict.org.il.