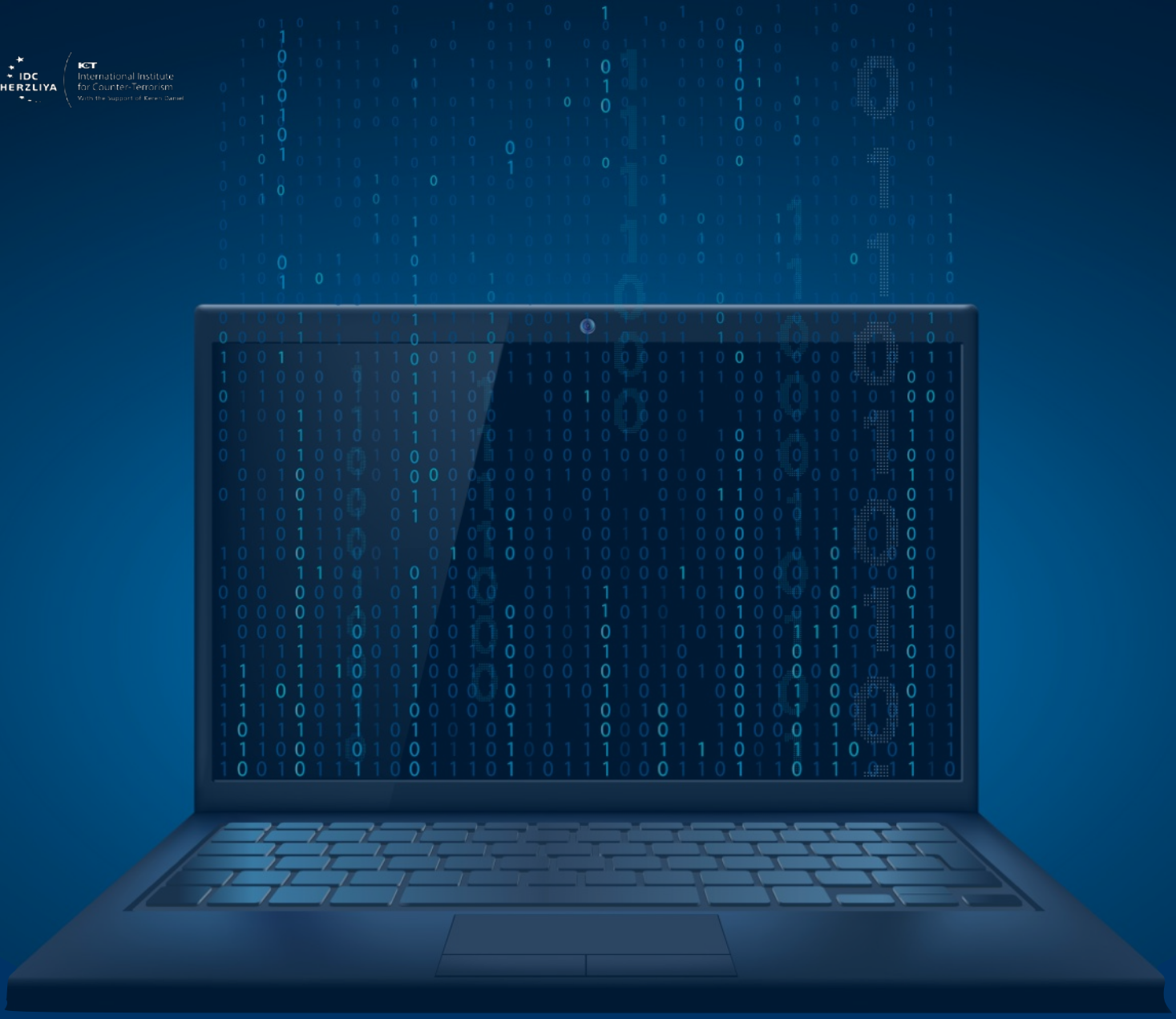
IDC HERZLIYA

ICT International Institute for Counter-Terrorism

With the support of Keren Daniel



Cyber Report 27

April-June 2018

Executive Summary

Cyber Report no. 27 by the International Institute for Counter-Terrorism (ICT) reviewed the prominent uses made of cyberspace by terrorist organizations and their supporters in April, May and June 2018. This is not an exhaustive list but rather an identification of the main trends as they arose from the field, and their analysis is divided into four areas.

A. In the operational domain, jihadist organizations continued to use cyberspace for a variety of needs, the most prominent among them being propaganda for the purposes of strengthening the media system, recruiting fighters, encouraging "lone wolf" terrorist attacks and fundraising campaigns.

B. In the defensive domain, there was no discernible significant innovation in the defensive use of cyberspace by terrorists. The trend of distributing content on issues of security and encryption, privacy and anonymity, warnings against phishing and the safe use of mobile devices continued.

C. In the offensive domain, terrorist organizations continued their efforts to improve their offensive capabilities but those capabilities are still undeveloped and remain at a low level, especially with regard to hacking into social media accounts or Web site defacement.

D. In the arena of international counter measures against cyber threats, a trend was identified in which subcontractors are used disrupt the communication activities of critical infrastructure. Security experts recommended setting a high standard throughout the critical infrastructure supply chain. Law enforcement operational activities continued to curb criminal activity on the Internet, and leading technology companies promoted cooperation to deal with terrorism-inciting content on the Internet.

Table of Contents

Operational Uses

In the operational domain, jihadist organizations continued to use cyberspace for a variety of needs, the most prominent among them being propaganda for the purposes of recruitment and fundraising campaigns. The following are documented cases:

Propaganda

- A group of Islamic State (IS) supporters called "Inghimasat Dawlawiya" ("Stormtroopers of the [Islamic] State"), which operates on social networks, published a call on IS supporters and members to renew their vow of allegiance to the Caliph, Abu Bakr al-Baghdadi.

A banner calling on IS supporters to renew their vow to Abu Bakr al-Baghdadi, the leader of the Islamic Caliphate

- IS supporters published several banners on Telegram calling on supporters to increase media activities on social networks against the enemies of Islam.

The title of the banner, "Jihad Fighter, You are a Media Man"

- IS supporters continued to spread threats to attack western countries and called for "lone wolf" attacks, while emphasizing that they are in a holy war against the forces of heresy. The month of April saw an increase in threats to attack the United States.

A banner posted to Telegram inciting to attacks on Americans

- The Rimah media group, which is involved in media for the IS, published an infographic on Telegram detailing its total media activities for the IS over the past six months. For example, it claimed to have published 84 designed banners, one book, and more.

An infographic by the Rimah media group detailing its media activities on behalf of the IS

- In the beginning of May, IS supports distributed banners on Telegram under a title drawn from a Quranic verse: "They are the Enemy So Beware of Them". The banners warned Muslims of spies and collaborators with the West, and demanded that they be exposed and executed.

A banner distributed by IS supporters encouraging the execution of collaborators and spies under a title drawn from a Quranic verse: "They are the Enemy So Beware of Them"

- In May, the IS continued to disseminate informational materials in several languages while using the American sharing site, archive. For example, Al-Nur media institution, which is responsible for publishing informational materials in French, published a file in PDF and DOC formats, in French, about the organization's achievements on various jihad fronts. The file is a transcript of a radio program that was broadcast on May 2 on Al-Bayan radio, which belongs to the organization.

A monthly report, in French, by the organization about its achievements in various arenas of jihad

- The Telegram account of Al-Nur media institution, which is responsible for published informational materials in French for the IS, published an infographic in French that presented the organization's military achievements in Afghanistan. For example, it published an infographic detailing the organization's total armed activities in Afghanistan from April 2017 to April 2018, stating that 1,291 people were killed during the year in Afghanistan. Another graph that was published showed the organization's total military activities in Afghanistan between January 4 and February 24, 2018.

Visual graphs in French that were published on Telegram detailing the organization's activities in Afghanistan, one referring to the period from January 1 to April 30, 2018 and the second referring to the period between April 2017 to April 2018.

- During the month of May, IS supporters published threats on social networks as well as calls on their supporters to continue the wave of terrorist attacks in western countries. According to them, the Crusaders, including the US and Europe, are waging a systematic war to weaken Islam and, to this end, are attacking Muslim lands and their Muslim residents. Therefore, it is necessary to carry out revenge attacks through rammings, stabbings, and the like. For example, a Telegram channel named "Muharriar al-Ansar" published banners encouraging the execution of terrorist attacks in Spain, the US and against the World Cup games set to take place in Russia in June 2018 (see photos). Alongside this, they published banners calling for the killing of Muslim clerics who support tyrant Muslim regimes, such as Salman 'Awda, a prominent Saudi cleric.

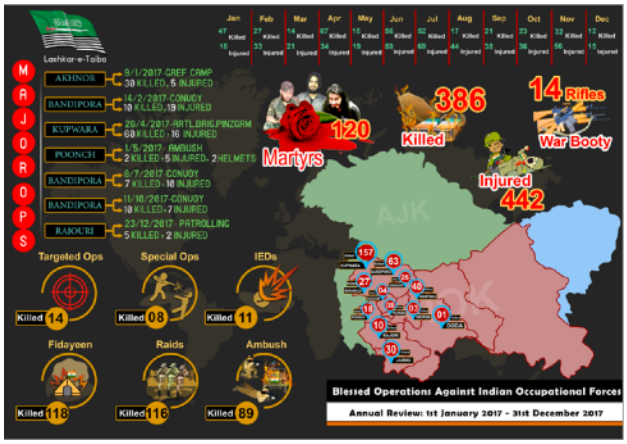
Banners calling for the execution of revenge attacks in France

Calls to attack the US and Europe under the heading, "We Will Slaughter You in the Streets After We Finish Slaughtering the Soldiers of Bashar [al-Assad] and his Collaborators"

- Al-Muhajireen media institution, which is ostensibly identified with the IS, announced on its Telegram channel that it had launched a Web site on the Internet. It stated that the purpose of the site is to spread the faith in the Oneness of God and life under His rule. The Web site itself operates in several languages – Arabic, Dutch, English, German, Farsi and Turkish – and includes a collection of tips on safe Internet surfing.

A banner published by Al-Muhajireen media institution on Telegram announcing the launch of a Web site

- The Pakistani terrorist organization, Lashkar-e-Taiba (LeT), launched a new digital magazine for propaganda purposes. The first issue of the magazine, *Wyeth*, included articles about chemical weapons, martyrdom, jihad, the role of women in the resistance in Kashmir, and a review of the struggle for freedom in 2017.



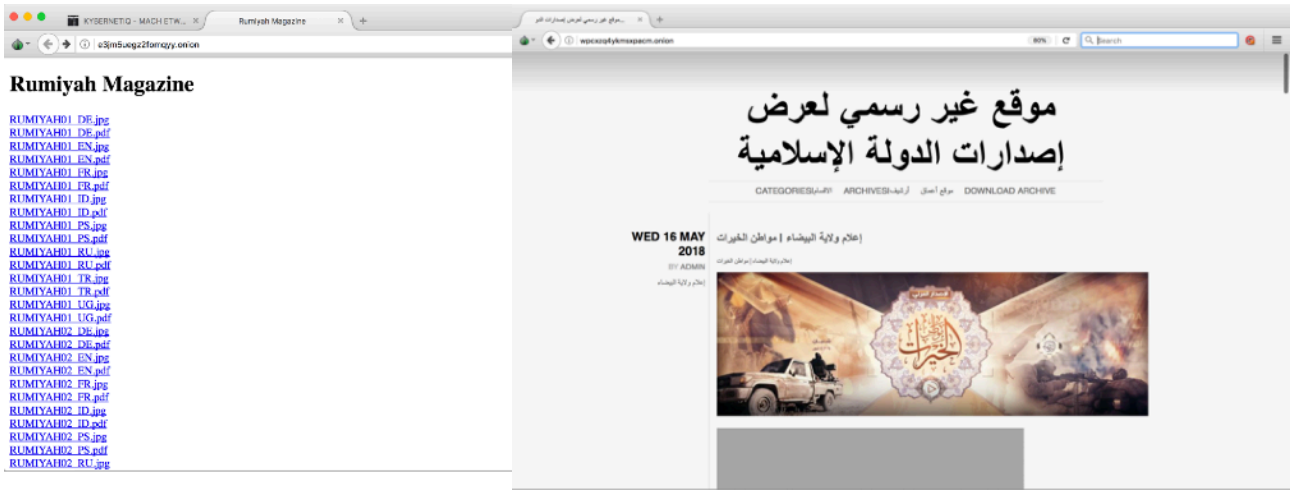
An infographic from Wyeth magazine

- The Dhakirat al-Ansar media group, which is involved in media for the IS, published an infographic in Arabic, English and Hindi that detailed its initial activity on social networks over the past 16 months. It stated that the group opened 9,635 Twitter accounts, 4,059 Facebook accounts and 346 Gmail accounts (Telegram, August 6, 2018).

The graph published by Dhakirat al-Ansar

Darknet

- IS propaganda materials were posted on sites on the darknet, including a dedicated site for the uploading of all issues of *Rumiyeh* magazine and a site for uploading videos. Both sites serve as archives for files and do not operate any other activity, such as forums.



Propaganda archives on the darknet

Recruitment

- Al-Nur media institution, which is involved in media for the IS in French, published a banner on Telegram calling on its supporters to "participate on the media front".

The banner of Al-Nur media institution

- The "Dawah and Guidance office" (Maktab al-Da'wa wal-Irshad) of Hayat Tahrir al-Sham, an umbrella organization composed of Salafi-jihadist factions in Syria, launched a campaign on May 10 titled, "Together to Paradise" in honor of the start of the month of Ramadan. According to the organization, the campaign was designed to spread the spirit of jihad and dawah among most liberated cities and villages in northern Syria. The campaign was launched on social networks and designated accounts were established for it on Twitter, Facebook, Telegram and WhatsApp. In addition, it was launched in Arabic, English, French and Uighur, which could indicate the presence of foreign fighters among its ranks. In addition, at the end of May 2018, the Dawah and Guidance office published a video documenting the reactions of people in Idlib to the above-mentioned campaign. All of those interviewed expressed great satisfaction with the campaign and noted its effectiveness.

A pamphlet distributed on Telegram by the "Students' Council for Shari'a in Al-Sham" to jihad fighters are checkpoints in Idlib

- The "Students' Council for Shari'a in Al-Sham", a rebel Salafi-jihadist organization in Syria, launched a campaign in the second half of May 2018 titled, "Message to a Nation" on its Telegram account. The organizers of the campaign sought to print a pamphlet that was published on Telegram, and to distribute it among the jihad fighters at the military checkpoints and patrols, as well as the patrol units in the Idlib area, in order to convey a message about the importance of their activities and their contribution to the defense of the residents of Idlib.

The campaign by the "Dawah and Guidance office" of Hayat Tahrir al-Sham

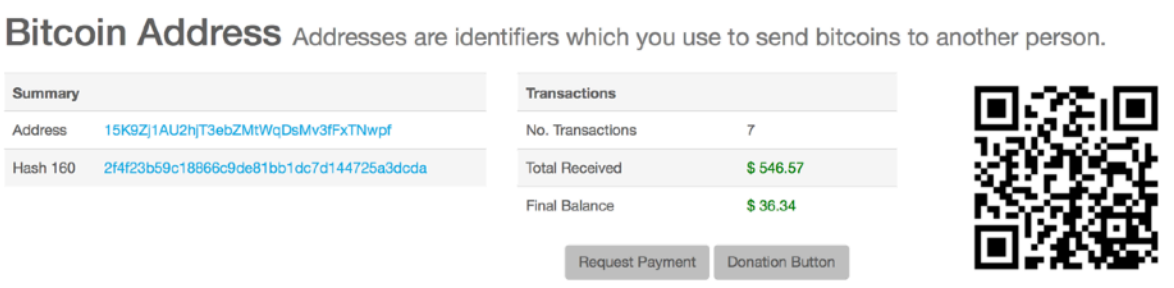
- A Hayat Tahrir al-Sham commander in Quneitra, Syria, published an announcement on the organization's Telegram account regarding the recruitment of new fighters to the organization who will undergo military training and will be educated according to Muslim law. The organization noted that registration will be held via a WhatsApp number between July 1-7.

An announcement regarding registration for a new round of recruits to the organization in Quneitra

Financing

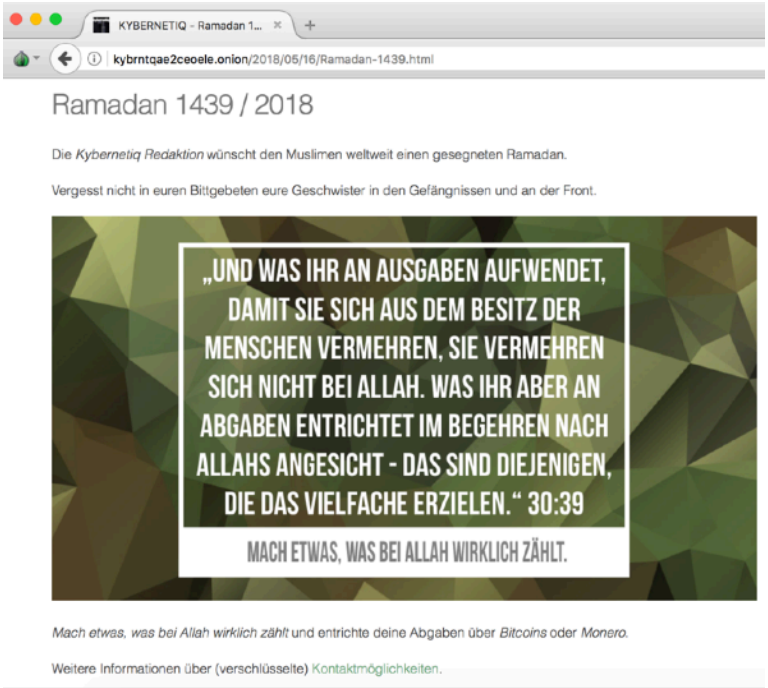
The use of the Internet for financing terrorism increased during the period under review. Some of the campaigns took the form of the publication and dissemination of calls for donations, and some used digital currency. The following are documented instances of financing campaigns that were identified during the period under review:

- A financing campaign on Telegram from May 25 by jihad fighters in Syria in honor of the month of Ramadan. The אל-צדקה group has operated financing campaigns using digital currency since December 2017 and defines itself as "an independent charity that supports the mujahideen in Syria". To date, the group's bitcoin wallet has received $546.57 in a total of seven transactions. During the month of June, the faction initiated another online fundraising campaign aimed at, among other things, purchasing new uniforms for jihad fighters. In the framework of the campaign, Gmail, WhatsApp and Telegram accounts were provided, as well as a "bitcoin" account. It also stated that the campaign receives assistance from the Abu Ahmed Foundation.



Above: Photos from the fundraising campaign; Below: A photo of the bitcoin wallet

- The "Kybernetiq" site is a Web site on the darknet (.onion) that distributes the cyber warfare magazine in German and is identified with jihadist elements. A fundraising ad was published on the site in honor of the month of Ramadan. It did not provide a bitcoin wallet, but one could contact the fundraisers using an encrypted email in order to receive the wallet.



A screenshot from Kybernetiq

- An online financing campaign using bitcoin by the Salafist Army of the Nation - a Salafist organization identified with Al-Qaeda in the Gaza Strip.

The banner of the campaign

- The Islamic Emirate of Afghanistan published a video and an announcement on its Telegram account calling for monetary donations to assist needy families in Afghanistan. For collecting donations, it published a WhatsApp number, a phone number and a Gmail address. The following is the text of the message:

  Just like the past year, the Department for the Affairs of Needy, Orphans and Disabled of the Islamic Emirate of Afghanistan had distributed food and monetary aid to the needy countrymen in Kandahar, Nimroz and Farah provinces.

  This department is designated by the Islamic Emirate to distribute aid to the needy families, widows, orphans and disabled strata of our society therefore all the Muslims who seek to help the poor and needy of our country in order to discharge their ethical and Islamic obligation, please contact the following address.

  Telephone: 0093700737054

  Whatsapp: 0093700737054

  Email: orphans.yia@gmail.com

  The latest video report about distribution of aid to the needy countrymen can be viewed and downloaded from here"

The video banner

Defensive Domain

During the period under review, there was no discernible significant innovation in the defensive use of cyberspace by terrorists. The trend of distributing content on issues of security and encryption, privacy and anonymity, warnings against phishing and the safe use of mobile devices continued. The following are several examples of documented cases:

Afaq Media Group

-The Afaq media group, which deals with increasing jihad fighters' awareness of the need to take security measures on the Internet, published the following:

- A list of free VPN services, such as Betternet, that violate the privacy of the user and trade his database for commercial purposes.

The VPN list

- An explanation regarding the installation of the Elementary OS on the computer as an alternative to Microsoft Windows.

The banner of the Elementary operating system

An announcement regarding the opportunity to join the ranks of the Afaq media group and assist it in the following areas: programming, design and ומנתאג. The group provided means of communication for this purpose via Telegram or WhatsApp.

The publication banner

- An announcement regarding the opening of a new Telegram channel that will archive video and audio clips published by the Afaq group.
- A collection of tips for the safe use of cell phones with the Android operating system, such as how to protect against KeyLogger; VPN installation; file encryption; a guide to locating and using fictitious phone to help register for various services on the Internet.

Defense basics in the Android system

- Guidebooks on various topics, such as use of the online store, Yalp; use of the encryption applications, Threema and Signal; a series of guidebooks on the safe and secure use of iPhones and iPads; use of the application, SUDO, which provides fictitious telephone numbers from different regions of the world to enable registration on social networks.

Examples of different banners

- Explanations regarding the use of the file encryption software, Vera Crypt; VPN services for the Windows system; a warning not to click on links posted on anonymous Telegram accounts since they are designed to identify the IP address of Web surfers. According to the group, all Web surfers must use TOR and VPN in order to make it difficult to identify user information.

A banner regarding the use of Vera Crypt

- The translation of an article that was published in Forbes on May 28, 2018 titled, "Rise of Computer Vision Brings Obscure Israeli Intelligence Unit into Spotlight". The translated article addressed the cyber capabilities of Unit 9900, which is responsible for visual deciphering, mapping and satellites.

GIMF

The technical department of the GIMF media institution, which belongs to Al-Qaeda, warned its users about a new application for Android devices called KevDroid, claiming that it is a spyware program that records conversations and steals personal information.

A warning not to use the KevDroid application

Offensive Domain

Terrorist organizations continued their efforts to improve their offensive capabilities, but those capabilities are still undeveloped and remain at a low level, especially when with regard to hacking into social media accounts or Web site defacement. The following are documented cases:

-A group of IS supporters called "Inghimasat Dawlawiya" ("Stormtroopers of the [Islamic] State"), which operates on social networks, published the following:

- Correspondence on Telegram calling on those interested in joining a course taught by the group on hacking into Facebook and Twitter accounts. It published a designated Telegram address for contacting the group.
- An infographic on Telegram in Arabic and English regarding its total media activities online. It stated that between November 2017 and January 2018, it set up 300 Twitter accounts, and between January 2018 to April 2018 it successfully hacked into 664 Facebook and Twitter accounts – 260 and 400 respectively.

An infographic regarding media and hacking activities

- In the beginning of April 2018, IS supporters noted that the organization's informational materials were accessible to download via Torrent. In addition, they noted that it is better to use VPN prior to downloading media material. Torrent is a unique communication protocol that enables the download of files (videos, games, etc.), allowing the user downloading the file from the Internet to also become a

source for other users who want to download the same file. Use of this protocol requires installation of the end-to-end Torrent software.

The banner regarding Torrent

Hacker Groups

-The UCC, which serves as an umbrella group for several hacker groups operating with the support of the IS, continued its effort to recruit hackers to its ranks. On the list of the UCC's member groups was a new group called Islamic Intelligence. To contact UCC leaders, interested parties were advised to use KEEMAIL.ME email, a service for sending encrypted emails.

Banners distributed by the UCC

International Counter-Measures

Coping with cyber-attacks requires global cooperation and out-of-the-box thinking. The following are steps that global players have taken in an effort to eradicate the phenomenon of cyber-attacks:

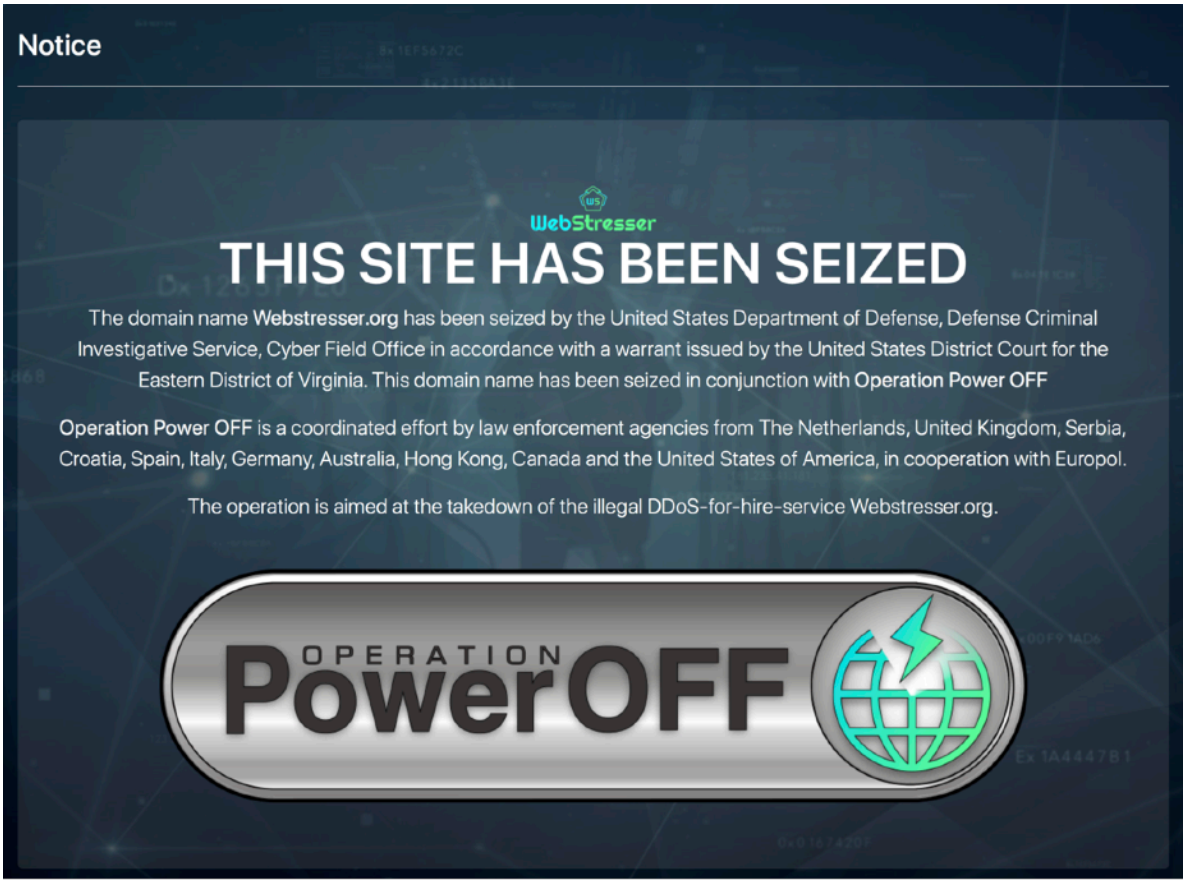
Critical Infrastructure and Subcontractors

- On April 4, several cyber-attacks in the United disrupted the communication networks of energy plants; the identity of the attacker is unknown. Hackers attacked a third-party company (subcontractor) that operates communications services for oil producers. The incident illustrates that hackers are attacking third parties related to critical infrastructure instead of attacking the infrastructure themselves, which are naturally better protected. Security experts recommend requiring subcontractors throughout the supply chain to meet the same high standards required of critical infrastructure.

Operational Activities

- Britain launched a campaign worth 9 million Euros to fight crime on the darknet. The initiative is directed against anonymous users on the darknet who commit crimes, such as the sale of hacking services, drug trafficking, weapons trafficking and human trafficking. Moreover, the campaign is aimed at embedding cybercrime units in local police stations.
- The FBI took control of a large botnet network that had spread to 54 countries and "infected" over 5000,000 "Internet of Things" devices. Preliminary research showed that the malware was activated by Russian groups whose aim was to sow destruction in Ukraine. The US Department of Justice listed the suspected groups; the Sofacy umbrella group, which includes the sednit, fancy bear, pawn storm, x-agent and sandworm groups. The US Justice Department also stated that it is committed not only to watching out for cyber threats, but to disrupting them and to using any means available to carry out this mission (May 24, 2018).
- European law enforcement agencies shut down a Web site that offered its customers cyber-attack services in the framework of "Operation Power OFF." The site, called webstesser.org, was operated by cyber-criminals and provided its customers with DDOS attack services; apparently the site's operators were involved in approximately six million attacks. The site had over 136,000 users who could carry out an attack at a cost of only 10 Euros. The structure and sophistication of the service allowed users without Internet or computer knowledge to successfully carry out cyber-attacks. The four operators of the site were ostensibly arrested in England, Canada, Croatia

and Serbia. The site was closed, and its infrastructure was seized by Germany and the United States, according to Europol.



A screenshot from the home page of the seized site

- England and the US accused Russia of the NotPetya ransomware attack that took place in 2017, beginning in Ukraine and spreading throughout the world. According to a White House statement, the ransomware caused billions of dollars' worth of damage throughout Europe, Asia and America. Moscow denied the accusations. NotPetya is a malware that paralyzes computers and computer systems if the ransom demand is not paid. The attack began against Ukrainian infrastructure, such as banks, airports and energy companies before it spread to 64 additional countries.

Technology Companies

- 34 technology companies, led by Microsoft and Facebook, signed an agreement on common principles titled, "The Digital Geneva Accord". The accord lists a set of principles, including a declaration that the signatories will not help any government – including the US government – launch cyber-attacks against innocent citizens and enterprises anywhere; the initiative reflects efforts by Silicon Valley to separate itself from government cyber warfare. The project was distributed among senior circles in the high-tech industry for weeks, and it requires companies to help any country that falls victim to a cyber-attack, regardless of geopolitical or criminal motive. Although the list of companies that signed the agreement is long, several companies have rejected signing it, including Google, Apple and Amazon.
- Technology companies added 88,000 "digital fingerprints" of terrorism-related content into a common database of companies. Those digital fingerprints can be used to block content before it is published. The Global Internet Forum to Counter Terrorism stated that this this was another step towards the target of 100,000 fingerprints of this type by the end of the year in Google, Facebook, Microsoft and Twitter forums, as well as smaller technology companies.

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

CYBER-DESK TEAM

Dr. Eitan Azani, Deputy Executive Director, ICT

Nadine Liv, Researcher, ICT

Dr. Michael Barak, Team Research Manager, ICT

Adv. Uri Ben Yaakov, Senior Researcher, ICT

CYBER-DESK CONTRIBUTORS

Adv. Deborah Housen-Couriel, Cyber security and international law expert

Oren Elimelech, Cyber Security Expert, Researcher & Consultant

Mr. Shuki Peleg, Head of Information Security and Cyber at MATAF, Israel

Dr. Harel Menashri, Research Fellow, ICT, & Cyber, Information Security & Technological Intelligence Expert, Israel

The research was facilitated by a special technology for the collection and analysis of information gathered from the DarkNet, developed by Athena from Mer Group in cooperation with SixGill.