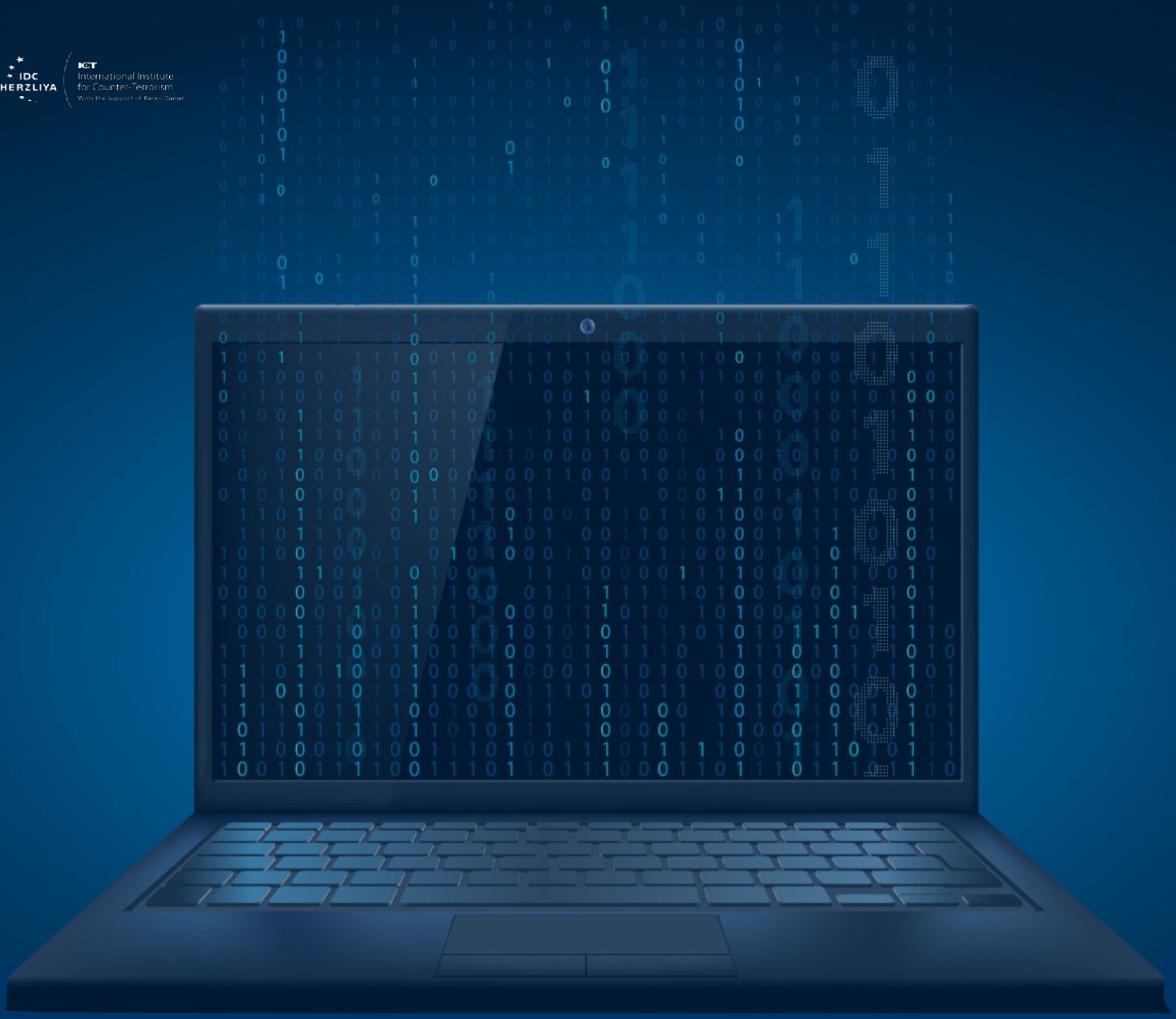
IDC HERZLIYA

ICT International Institute for Counter-Terrorism

With the support of Keren Daniel



Cyber Report 28

July-September 2018

Executive Summary



In the operational domain, jihadist organizations continued to use cyberspace to promote propaganda for operational purposes, including strengthening of the media campaign, recruitment of activists and encouragement for "lone wolf" attacks. Particularly prominent during this period was a new online campaign encouraging biological terrorist attacks.



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.



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, in our assessment, especially with regard to hacking social media accounts or Web site defacement. During the period under review, a trend was identified of recruiting hackers to sub-groups of the UCC collective; most of which were Indonesian in origin.



In the domain of global counter-measures against cyber threats, we identified a trend of expanding the use of technological systems in the fight against terrorism, including blockchain technology, facial recognition and artificial intelligence. In addition, documents, research and memos on terrorism in general, and cyber terrorism in particular, were published.

Table of Contents

1. Operations 4

1.1. Propaganda 4

1.2. Financing 7

1.3. Recruitment 8

2. Defense 9

2.1. Guidebooks 9

2.2. Warnings Against Forgeries 17

3. Offense 18

3.1. Prominent Hacker Groups 18

FMCC 18

Anshar Caliphate Army 19

UCC 21

3.2. Cyber-Attacks 22

4. International Counter-Measures 27

4.1. Technological Systems 27

4.2. Blockchain 28

4.3. Biometric Identification 28

4.4. Legal Aspects 29

4.5. Publications of Official Documents and Opinions 31

1. Operations

Terrorist organizations continued to use cyberspace for a variety of needs, with emphasis on the use of various social networks as a platform for the dissemination of propaganda messages, radicalization, recruitment and financing.

1.1.Propaganda

During the period under review, terrorist organizations continued to disseminate propaganda with the same characteristics as in the past. However, the number of publications that were disseminated on various platforms began to decrease. The following are several examples of propaganda content:

- Hayat Tahrir al-Sham, a Salafi-jihadist rebel organization in Syria, announced on its Telegram account the opening of a course on using the Adobe software to design and market content. According to the details of the program, the course took place over 20 hours during a period of three weeks, cost $75 and took place in the city of Idlib. In addition, the contact details of those running the course via Telegram, WhatsApp, Facebook and telephone were published.



A poster that was uploaded to the Telegram account of Hayat Tahrir al-Sham, announcing that registration for the Adobe course was open

- In the beginning of October 2018, Islamic State (IS) supporters launched an online campaign titled, “Campaign to Encourage the Residents of the Arabian Peninsula”. According to the initiators of the campaign, its goal was to distribute publications in praise of the Islamic

Caliphate among residents of the Arabian Peninsula and to encourage them to fulfill the commandment of jihad.



- The Tubath jihadist media institution, which belongs to Hayat Tahrir al-Sham, appealed to its supporters to join an online media campaign to disseminate its accounts on social networks and to participate in design courses as an informational tool (see photo).



Tubath Jihadist media institution

- In July 2018, IS supporters launched the hashtag, “to my assisting brother" about the importance of taking part in the organization’s media efforts. At the outset, the organization called on its supporters around the world not to restrict propaganda for the organization to the Telegram platform alone, but to expand it to other social networking platforms, such as Facebook, Twitter,

YouTube, Instagram, etc. It also stated that it is better to plant the organization's messages on the public accounts of government officials, journalists, senior clerics and more. Finally, it presented a long list of Twitter accounts belonging mainly to Saudi government and religious officials.

- A campaign was launched on an IS-supporting Telegram group, calling for bioterrorism and accompanied by the hashtag, #Bio_Terror. In the framework of the campaign, an infographic was published about Petalominium, a bacterium that kills the victim after 24 hours due to an incurable injury to the chest, including an explanation of how to produce פטלומיניום for use as a biological weapon. It also published a video calling on IS supporters living among the infidels to revive the nightmare (a reference to the September 11, 2001 terrorist attacks) in the countries of Satan worshippers using quiet and destructive weapons that cannot be detected or identified, and which cannot be avoided. With simple equipment, viruses and infectious bacteria can be produced and safely dispersed in three simple steps. First, the most severe epidemics must be found. Second, the bacteria should be dispersed in accordance with its classification. Third, care should be taken to avoid injury that may occur when preparing hazardous materials (August 3, 2018). It should be noted that the biological terrorism campaign was launched after the deadly ricin poison case in Cologne, Germany, was exposed in June 2018. In this case, German security forces uncovered a bioterrorism case centered on a radical Tunisian activist suspected of having contacts with the IS. This case was the first time a jihadist terrorist in the West had succeeded in producing a biological toxin. The case underscores the threat posed by bioterrorism in Europe, and the importance of electronic surveillance in exposing plots by extremists using the Internet to acquire deadly materials.[1]

[1] https://ctc.usma.edu/app/uploads/2018/08/CTC-SENTINEL-082018.pdf



Publications from the #Bio_Terror campaign

1.2. Financing

- Hayat Tahrir al-Sham launched an online fundraising campaign to finance the fortification of Idlib against a planned attack by Syrian regime forces and its allies. Banners were distributed on social networks on the topic, and a Telegram account and telephone number for donations were published.

- In August 2018, the Jihad's Callers Center" an umbrella organization of Salafi-jihadist clerics in Idlib, launched an online fundraising campaign for the needy on social networks in honor of Eid al-Adha. The banner that was published stated that the price of camels and cattle was $1,000 dollars and the price of sheep was $150.



The banner by Hayat Tahrir al-Sham

1.3. Recruitment

- The military department of Hayat Tahrir al-Sham launched an online campaign to recruit residents of Idlib to a new military unit called the "Red Bands" or the "death squads" (/ al-'Asa'ib al-Hamraa). In the framework of the campaign, contact information was provided, including a telephone number and dedicated Telegram account. In addition, the organization launched an online campaign to recruit manpower for medical teams.



From left to right: a banner calling for the recruitment of manpower for medical teams; banners calling for recruitment to the death squads

- Sheikh Abdullah al-Muhaysini, a senior Salafi-jihadist cleric in Syria, announced the launch of an online competition called, "The Journey of Eternity" (Rihlat al-Khulud) about the world to come. Al-Muhaysini called on followers of his Telegram account to listen to his speeches, which were uploaded in videos to YouTube, and to answer two short questions about the speeches that appear at the end of the video. According to him, those who correctly answer the questions via the WhatsApp or Telegram accounts, whose addresses were provided, were promised the following prizes: 1. gunpower; 2. a gold ring; 3. $200-1,000; 4. a cell phone.



The announcement of the launch of the online competition

2. Defense

Terrorist organizations are aware of the efforts of security agencies and the activities of prominent players on the Internet in general, and on social networks in particular, to remove jihadist content from their platforms. Therefore, terrorist organizations continue to disseminate guidebooks and instructions, and to move to the darknet where they claim to be able to protect the movement and anonymity of the organizations themselves, as well as their supporters, from the surveillance programs of security agencies and activists operating against terrorist organizations on the Internet.

Organizational support for cyber defense continued with the translation of guidebooks distributed by non-terrorist entities (technology manufacturers), and the independent production of manuals, instructions and warnings about malware.

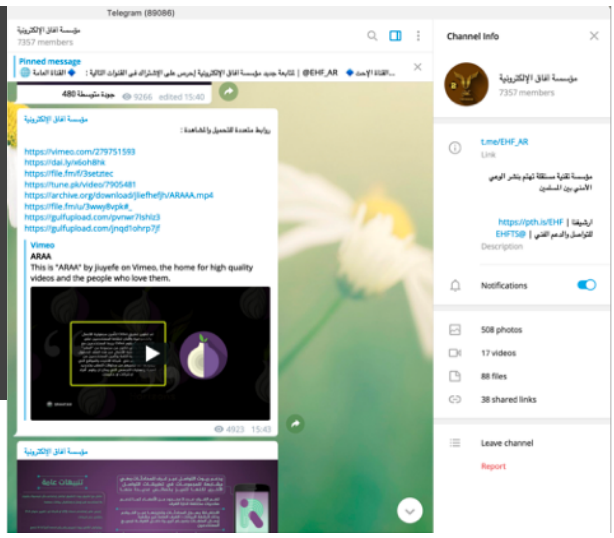
2.1. Guidebooks

During the months of July-September 2018, the Afaq jihadist media group, which is involved in raising the awareness of jihad operatives to take security measures on the Internet, published dozens of guidebooks, including the following:

- Guidebooks on the topics of: safe use of the WhatsApp messaging program; Tor; Firewall; file encryption on an Android device; Riot; VPN services; use of fake telephone numbers for Android devices; an explanation the Conversations application; use of the RIOT social network application; use of the Threema social network application; an explanation about the use of the Zom application for encrypted communication; a comprehensive guide to safe and secure use of Android and iPhone devices; a video explaining how to install the Orbot application on Android devices through which one can change the IP and protect users from surveillance on the Internet and more.



A banner encouraging the use of the social network application, Threema



Links to an instructional video on installing Orbot

- An announcement regarding the new possibility of joining the Telegram channel team with regard to programming, design and editing. The announcement included contact details via WhatsApp, Telegram and Threema.



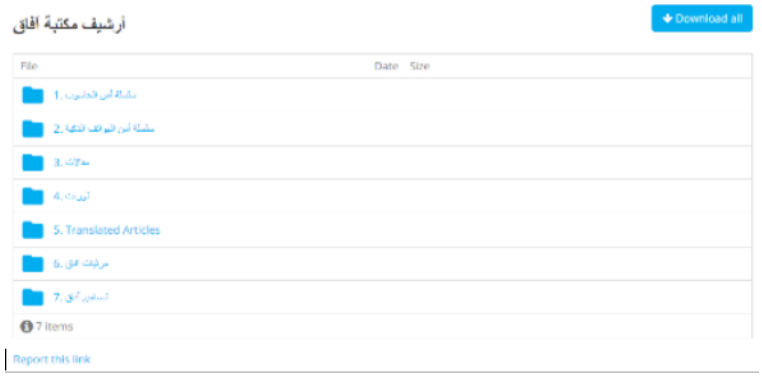
The Announcement regarding the new possibility of joining the programming, design and editing team

- A warning against surfing on the al-Ansar Web site, claiming that it is a phishing site designed to steal information about identification details on social networks.



A warning about a phishing site

- An announcement regarding the launch of an online archive of all publications by the Afaq media group.



The launch of the archive

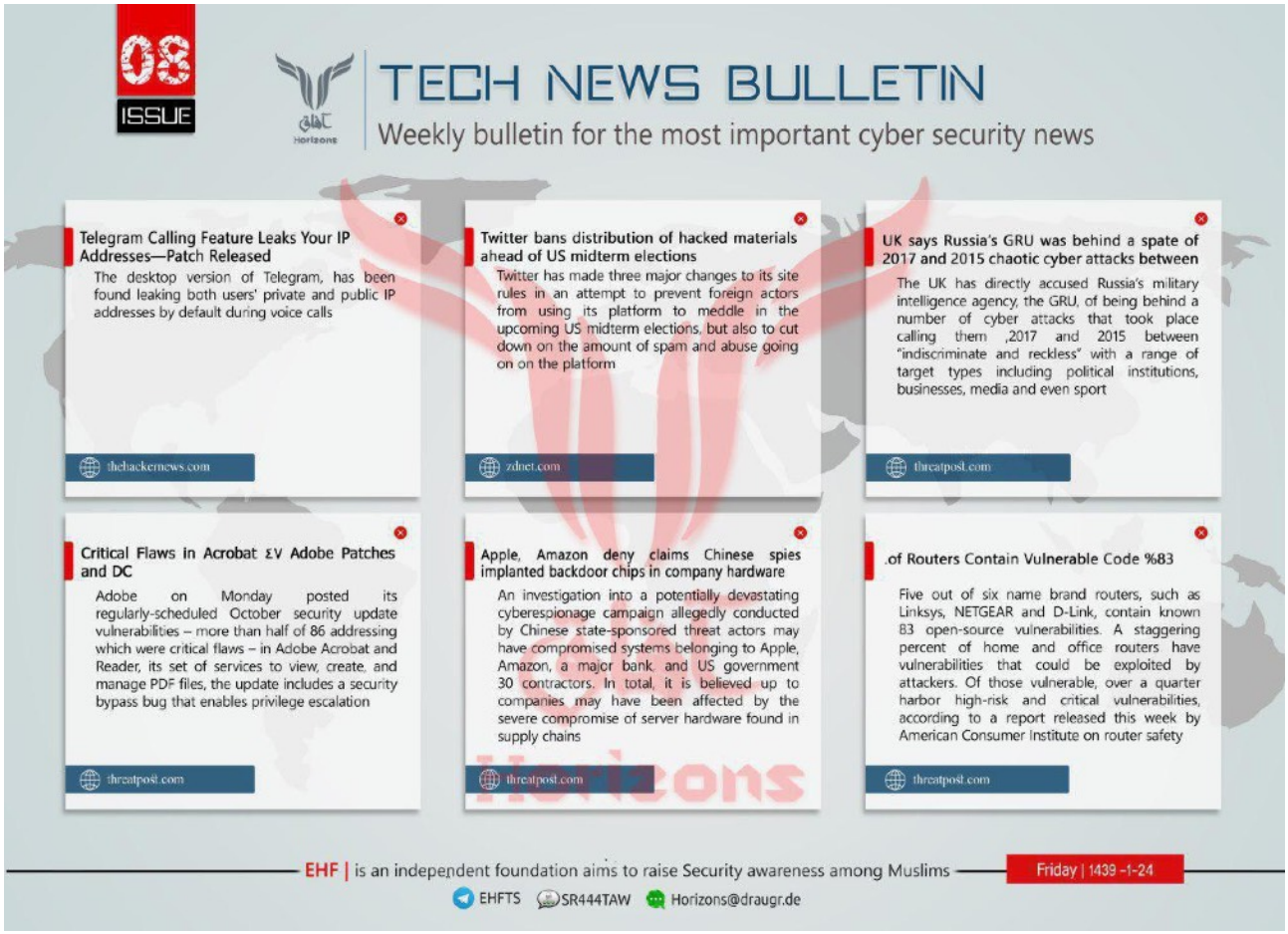
- An announcement regarding the security measures to be taken concerning the application, “The Mujahid’s Security” (Amn al-Mujahid), which serves as an encrypted chat software among jihad operatives. The beginning of the announcement stated that many jihad supporters face challenges regarding security on the Internet, especially security breaches of messaging software. It stated,

"Given the weakness of the technical team in this field, surveillance of [jihad] supporters using the Internet has become easier. Therefore, we have an obligation to publish this clarification regarding the gaps that governments and intelligence agencies may exploit. Later in the announcement, the group referred to a security gap in the encryption software in the PGP protocol, which enables an attacker to access email addresses, make changes to them and encrypt them in html before they reach their destination. The group then noted that the "Mujahid's Security" application was developed by the "Markaz al-Fajr lil-'Ilam" (which belonged to Al-Qaeda) at the end of 2013 in response to the Edward Snowden leaks about the use of the PGP protocol to encrypt messages. According to the group, many jihad supporters use this application but since the Markaz al-Fajr lil-'Ilam stopped operating, the application has not been updated and its official site has not been removed. This situation enabled governments and intelligence agencies to encrypt the application and use it as a tool to monitor and spy on jihad supporters. Despite the exposure of this security breach, the Markaz al-Fajr lil-'Ilam did not bother to clarify to supporters the extent of its impact on the "Mujahid's Security" application. In light of this, the group suggested that supporters use open sources to encrypt the PGP protocol, such as the Openkeychain application, as an alternative to the "Mujahid's Security" application" until the Markaz al-Fajr lil-'Ilam publishes a clarification on the matter, as five years have passed since the application was developed without updates or security tests.

- The "Tech News Bulletin", a weekly bulletin for the most important cyber security news, was launched. Among the bulletin news headlines that appeared in the first issue: ADOBE adds important security improvements to four of its products; Extensive breach of Instagram; Warning about a security breach in PHP commands on WordPress blogs; Google can find the location of a Web surfer even if the latter closed the location setting option; A plan to convert former fighters in the British army to "electronic fighters"; The Mozilla company responsible for the Mozilla browser violates the privacy of users. Among the bulletin news headlines that appeared in the

second issue: The opening of the Australian Cyber Security Center in Canberra; Facebook uses artificial intelligence to predict user activity based on a leaked document; In Australia there is a ten-year prison sentence for anyone who refuses to open his cell phone; ADOBE adds security improvements to the PhotoshopCC software; The EU gives social networks a maximum of one hour to remove "terrorist" content; Apple forces Facebook to remove the VPN application from the App Store. Among the bulletin news headlines that appeared in the third issue: An important change in the Telegram network's privacy policy; CIA network exposed in China due to the use of unsecured media; Instagram adds the 2FA system to enhance user privacy; Yahoo still analyzing email messages for advertising purposes; The Cobalt hacker group attacks Eastern European banks; RCE breach strikes APACHE system and enables hackers to gain control of many network servers. Among the bulletin news headlines that appeared in the fourth issue: MCAFEEE company admits that its special electronic wallet is vulnerable to hacking; Five Eyes countries ask technology companies to build backdoor access to their unique encryption protocols; 400,000 Web sites risk being hacked due to a git-based system; Google secretly tracks your shopping list by using a Mastercard card database; Launch a new version of the Tor browser. Among the bulletin news headlines that appeared in the fifth issue: A European court rules that mass surveillance by the British government violates human rights; US charges North Korean spy over WannaCry and Sony Pictures hack. Among the bulletin news headlines that appeared in the sixth issue: Tracking PEGASUS spyware in 45 countries; Laws regarding opening code in the US; Violent virus found in a ransom request software in Windows and Linux. Among the bulletin news headlines that appeared in the seventh issue: US unveils a new cybersecurity policy; Facebook claims that at least 50 million accounts were hacked after hackers exploited a security breach on the Web site; France records a large jump in the number of complaints against the European data protection law; Twitter warns users about leaks of direct correspondence. Among the bulletin news headlines that appeared in the eighth issue: Critical

flaws in Acrobat eV Adobe patches and DC; 83% of routers contain vulnerable code; Apple, Amazon deny claims Chinese spies implanted backdoor chips in company hardware; Telegram calling feature leaks your IP addresses – patch released; UK says Russia's GRU was behind a spate of chaotic cyber-attacks between 2015 and 2017.



Issue no. 8 of the Tech News Bulletin

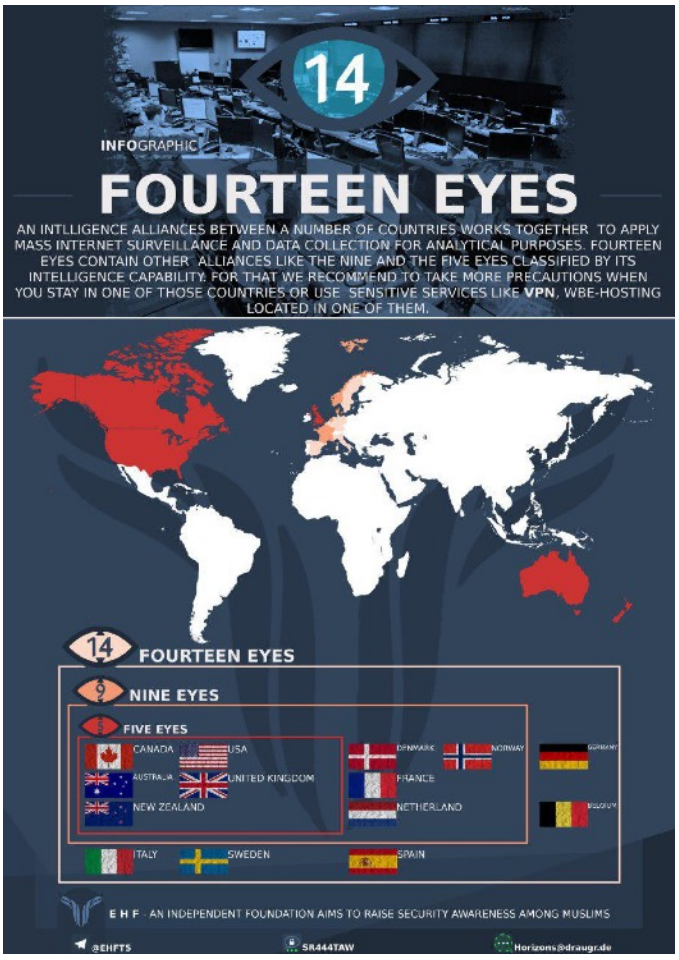
- Greetings to members of the Muslim Nation and jihad fighters on the occasion of Eid al-Adha. In the announcement, the group emphasized that the correct path is one of jihad and Paradise, where martyrdom will lead them, and it praised jihad fighters wherever they operate.

- A video demonstrating how to remove the camera and microphone from Android devices as a means of protecting against potential attackers. According to the group, the purpose of removing them is to prevent the enemy's intelligence agencies from spying jihad supporters.



The video banner

- An announcement titled, "Fourteen Eyes", which referred to the cooperation between the intelligence services of several Western countries aimed at intelligence gathering and analysis. In light of this, the group warned that greater caution should be exercised in the following countries: the US, Australia, England, New Zealand, Canada, France, Holland, Denmark, Norway, Italy, Sweden, Belgium and Germany (see photo).



The "Fourteen Eyes infographic

- Al-Badr media group, which is involved in media for AQAP, published an article regarding the advantages of using the Tor encrypted chat software.[2]



The article banner

- An IS-supporting group promoting programming education as a basis for successful hacking published an essay, which serves as the introduction to a book due to be published on the topic of hacking (August 9, 2018).[3]



The banner of the book's introduction. Source: Site

[2] 7.7.18. http://www.alfidaaforum.net/vb/showthread.php?t=123193 ; https://risala.ga/l6yi/

[3] https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/is-linked-group-promotes-education-in-programming-as-precursor-to-successful-hacking.html

2.2. Warnings Against Forgeries

- The UCC collective of IS-supporting hackers published warnings on its Telegram channel of fake publications on the Internet that are ostensibly done on its behalf. The group warns against all types of electronic publications, including text, audio and video, which are not distributed on the group's official channel. It also recommended that IS supporters be very careful and pay attention to the content published by impersonators attempting to hack the supporters' computers, and therefore links from suspicious sources must be checked carefully before clicking on them.



The warning published by the UCC group. Source: Telegram

- An IS-supporting Telegram group published a warning about a Telegram account that turned out to be fake (see photo below). The post was accompanied by text asking viewers to beware of the fake channel, along with the hashtag #warning (July 1, 2018).



From left to right: a screenshot of the warning; a screenshot of the fake channel

3. Offense

Terrorist organizations continued their efforts to improve their offensive capabilities but at this stage it seems that they are lacking significant technological capabilities in this field. Nevertheless, it should be noted that these organizations may hire external parties, such as those who identify with .terrorist ideas or online crime, or acquire these capabilities from terrorist-supporting states

3.1. Prominent Hacker Groups

FMCC

- The FMCC is part of the IS-supporting hacker collective, United Cyber Caliphate (UCC), and its members seemingly originate from the Southeast Asia region. The group has been active since 2017, and has disseminated videos and banners to recruit more hackers to its ranks. The incident with which the FMCC is most identified is its attempt to imitate the Wannacry ransomware in May 2017.[4]
- On July 9, 2018, the FMCC published a video in which it called on lone wolves and hackers to join the group in order to fight against the infidels and inflict terrorism on the world. The video showed a protonmail (encrypted email) address through which one can contact the leader of the group.





Screenshots from the video

[4] https://www.ict.org.il/Article/2096/cyber-report-no-22#gsc.tab=0

- In addition, the FMCC published a screenshot on its Telegram channel of a Web site that it had hacked and defaced (July 9, 2018). The content included the logo of the UCC collective alongside a declaration of the organization's intentions to attack targets in cyberspace and the physical world. The caption also listed the names of the groups affiliated with the collective as of the date of the breach: 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.



A screenshot on the Telegram channel of the FMCC group

ANSHAR CALIPHATE ARMY

- The IS-supporting hacker group, Anshar Caliphate Army, is part of the UCC collective. The group was first documented in June 2018 in Telegram groups in which it declared itself as one of the groups active in the framework of the UCC umbrella organization. Content and language analyses reveal that the origin of this group is Indonesian.



A digital poster of the Anshar Caliphate Group

- In July, the group distributed a banner in which it told Facebook founder, Mark Zuckerberg, to "go to hell". In the background of the banner was an image processing of Zuckerberg's face alongside headless body (July 4, 2018).

- Shortly after this publication, the group published a collage on its Telegram channel containing screenshots of a large number of hacked accounts on social networks.

- The following month, the group published a video appealing to IS supporters in Indonesia to join its campaign and carry out cyber-attacks against the Indonesian government and social media accounts. The attacks were set to be carried out on August 17 and was called #OpTheWorld. This campaign began in June 2018 (August 16, 2018), according to our estimates.[5] These activities apparently stemmed from the Indonesian government's decision to block the social media accounts of IS-supporting groups.[6]



Top left: screenshots of hacks into social media accounts; top right: the banner threatening Zuckerberg; Bottom: a screenshot from the video

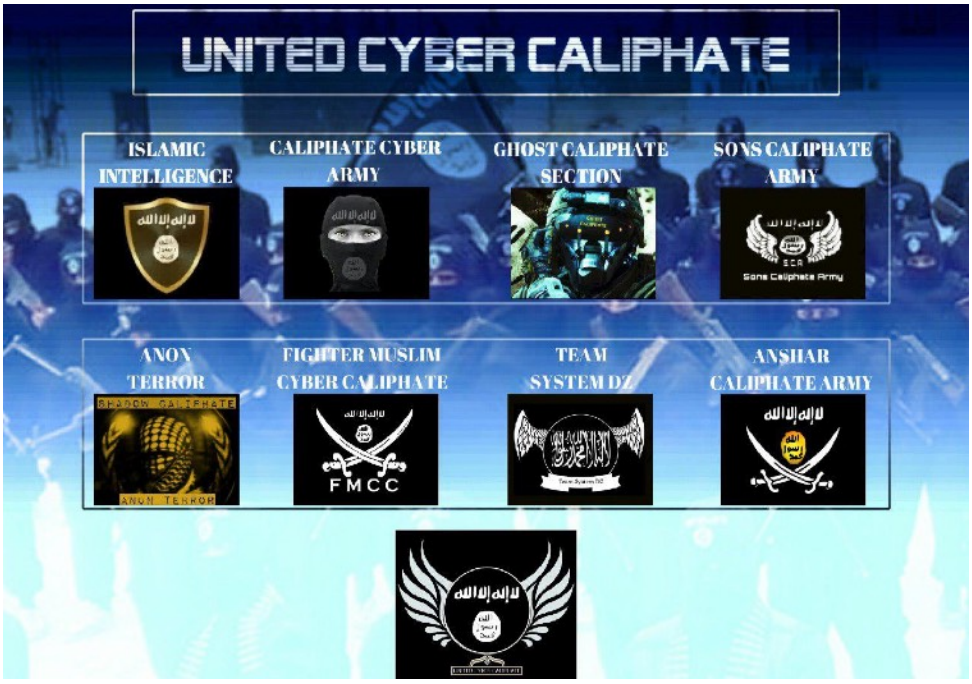
[5] https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/anshar-caliphate-army-release-video-threatening-indonesian-government-with-cyber-attacks-on-aug-17.html

[6] https://www.channelnewsasia.com/news/asia/pro-islamic-state-hackers-threaten-terror-attacks-against-10644690

- In addition, the group vowed to kill hackers from the "Anonymous" collective, which is waging a prolonged cyber campaign against the UCC and bringing down its accounts (September 28, 2018).[7] In a Cambridge University report published in 2017, a warning was issued that as long as the IS continues to develop into a virtual caliphate and enlist talented technology enthusiasts, the group's hackers will be able to attack critical infrastructure. In the hands of IS-supporting cyber groups, even defective spyware can be used to maximize publicity, disrupt business continuity, and frustrate security agencies and the general public.[8]

UCC

- The UCC collective published a digital poster on its Telegram channel detailing the composition of its members (July 9, 2018). The poster accompanied a publication listing the Web sites that UCC activists claimed to have hacked. The poster listed the following groups as members: Islamic Intelligence, Caliphate Cyber Army, Ghost Caliphate Section, Sons Caliphate Army, Anon Terror, Fighter Muslim Cyber Caliphate, Team System DZ, Anshar Army.



The poster published by the UCC

[7] https://pjmedia.com/homeland-security/cyber-caliphate-vows-to-kill-anonymous-hackers-who-have-been-taking-down-isis/

[8] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/pool-re-cyber-terrorism.pdf

3.2. Cyber-Attacks

- The UCC collective published an infographic in which it reported the cyber-attacks that were carried out by the group over a 70-day period. The attacks included 770 DDoS attacks, the hacking and destruction of over 900 international sites, and the hacking of over 1,500 social media accounts. The groups that participated in these 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 distributed on a Telegram channel in Arabic and English, and was accompanied by a statement, according to which most of the attacks mentioned in the infographic occurred in East Asia and in the framework of the #OpTheWorld cyber campaign (August 28, 2018).



The infographic published by the UCC

- The UCC collective published (July 9, 2018) an announcement according to which, 21 days following the attack on East Asian countries, the hackers of the Caliphate hacked at least 213 Web sites in Thailand, the Philippines, Indonesia and South Korea. In addition, members of the group brought down close to 530 sites using DDoS attacks. Later in the announcement, it stated that over 700 social network accounts were hacked, most of them belonging to military personnel among Muslims who had become corrupt and Crusaders in these areas.



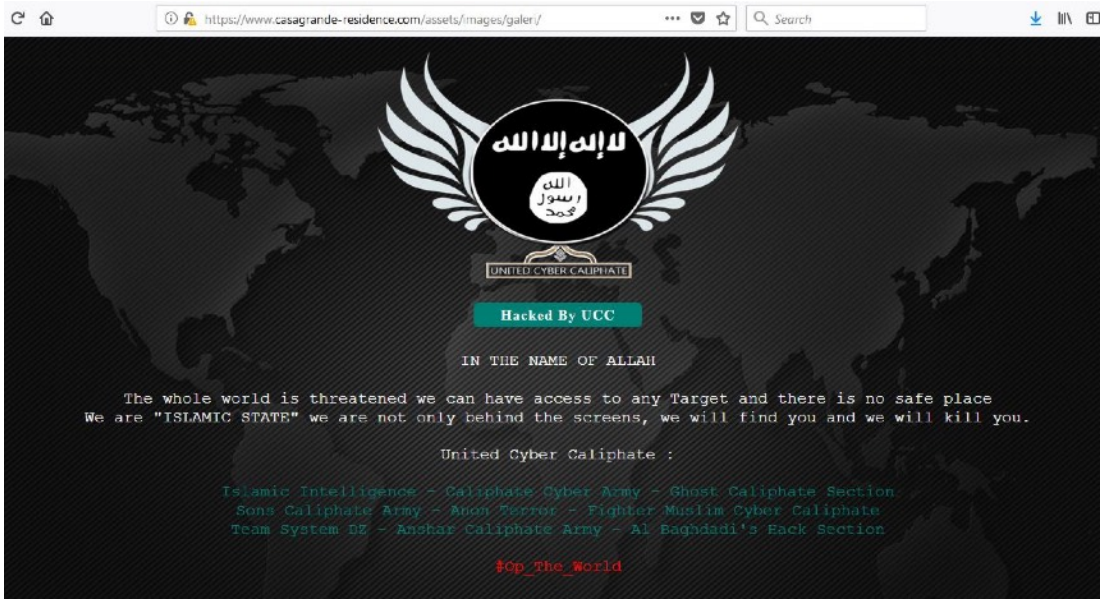
The announcement published by the UCC

- The Anshar Caliphate Army group published a poster in which it listed the cyber-attacks that it claimed to have carried out between May and July 2018 in the framework of #OpTheWorld. It noted 160 Web sites that were defaced, as well as 110 Facebook accounts and 20 Instagram accounts that were hacked. The attacks were directed at sites and accounts from a range of countries: India, Canada, Russia, England, the US, Israel, Holland, Germany, France, Brazil, Indonesia, Taiwan and China (July 27, 2018).



The announcement published by the Anshar Caliphate Army

- The IS-supporting UCC collective claimed to have brought down commercial and economic Web sites belonging to the "infidels", causing severe economic loss (August 27, 2018).[9]



A screenshot from the defacement attack carried out by the UCC

- The UCC collective published a banner calling for the launch of a cyber war against the infidels. The banner was distributed on Telegram channels and accompanied by text in Indonesian (August 8, 2018).



The banner published by the UCC

[9] https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/hacking-subdivision-of-pro-is-military-focused-media-group-claims-taking-down-websites.html

- The UCC collective published a statement by the leadership of the Caliphate Hackers Union, which contained a joint announcement by the leadership of the Caliphate Hackers Union, the "Caliphate Cyber Army", the "Kalachnikv" group, and the "Sons Caliphate Army" regarding their renewal of activities for the Islamic Caliphate. These activities, according to the announcement, will focus on attacking and terrorizing the enemy. Alongside this announcement, the hacker groups praised those Muslims in the West who are willing to sacrifice their lives and carry out lone wolf attacks for the Caliphate and for Islam. At the end of the announcement, they emphasized that the groups have no social media account other than one official channel, to be announced.



The announcement published by the UCC

- In July, it was reported that Lebanese security agencies, and several government bodies and private institutions fell victim to attacks by hackers who stole information and sold it to third parties that have not yet been identified. The campaign was described as the largest hacking attack in Lebanon's history.[10] Since it was reported that several Lebanese suspects had been arrested, it is possible that the attacks were carried out by criminal elements or by an organization such as Hezbollah.

- In early June, several Telegram channels associated with Al-Qaeda in Syria, such as the Telegram channel "General Mujahideen Service", announced a new opportunity to register to a Telegram channel called "Report on [Telegram] Channels" in order to join the "Electronic Jihad Army". The purpose of the channel is to coordinate activities between members and new registrants to remove channels with Shi'ite content. In addition, it invited visitors "to participate in the removal of Telegram channels belonging to Shi'ites and their allies". In another correspondence, hackers in the "Electronic Jihad Army" were asked not to settle for reporting Telegram channels with Shi'ite and Alawite content, but also to hack and destroy them.



A call to join the Telegram account in which activities to remove Telegram channels will be coordinated

[10] http://www.naharnet.com/stories/en/248204-report-lebanon-s-security-agencies-large-firms-hacked

- The Colbalt Dickens hacker group, which is tied to the Iranian government, attacked the Web sites of British universities and academic institutions around the world as part of a widespread campaign aimed at stealing confidential research and intellectual property.[11] The hackers attacked 76 universities in 14 countries, including Australia, Canada, China, Israel, Japan, Switzerland, Turkey, England and the US. Some of the universities appear on the Times' list of the top 50 universities in the world. The attack included the creation of a fake site with a similar appearance to the login page of each university. Anyone who mistakenly entered their account details and password on the login pages of the fake site actually gave their identification information to the hacker group. The victims of the attack were then connected to the authentic site without being aware that they had fallen victim to a cyber-attack.

4. International Counter-Measures

Coping with cyber-attacks requires global collaboration and out-of-box thinking. The following are steps taken by global players in the framework of the effort to eradicate the phenomenon of cyber-attacks:

4.1. Technological Systems

The use of technological tools has many advantages. Tasks performed using technological means tend to be faster, more efficient and more accurate than those performed by humans. Similar to the use of various technologies in the media or in medicine, for example, technology can be harnessed for national security.[12] In the coming decade, technologies will play a significant role in national security.[13] The following are several technologies with the potential to influence our security:

[11] https://www.independent.co.uk/life-style/gadgets-and-tech/news/iran-hackers-uk-university-cyber-attack-security-cobalt-dickens-a8506406.html

[12] https://www.british-business-bank.co.uk/wp-content/uploads/2018/07/HMG-NS-Technology-AOIs-Summary_v0.1.pdf

[13] https://www.dhs.gov/sites/default/files/publications/2018_AEP_Emerging_Technology_and_National_Security.pdf

4.2. Blockchain

- Blockchain is a technology that serves as a distributed account ledger used in computer networks that documents transactions in real time. Blockchain has potential implications for many areas, including financial services, health systems, information storage and even national security. For example, Blockchain can change the supply chain to defense contractors. Components of defense systems are manufactured worldwide. In cases where the supplier is close to a foreign government, there is concern that the supplier will install surveillance or backdoors. Use of the Blockchain technology may reduce the risk by carefully monitoring the products of each subcontractor.[14] In addition, Blockchain can securely manage the identification of government employees and contractors; thus, security classification can be done through Blockchain. The government can also use Blockchain to secure interorganizational communication and improve the storage of digital files.

- The European Union published a study on Blockchain, bitcoin and their use for the purposes of cyber-crime and terrorism financing. According to the document, the problem is significant. Although the extent of misuse of virtual currencies is unknown, its market value is estimated at over €7 billion worldwide. The document was prepared by the EU Policy Department, which described the phenomenon from a legal perspective, focusing on the use of virtual currencies for economic crime, money laundering and tax evasion. In addition, the document included recommendations for European regulations (July 2018).[15]

4.3. Biometric Identification

- Biometric technologies for facial recognition have been creating a "buzz" recently. For instance, biometric technology for facial recognition is now a standard feature in the iPhone X and replaces the fingerprint scanning in earlier models. Even though the technology is still in its

[14] See ICT Cyber Reports from April-June 2018 on the topic of subcontractors and the danger posed by them.

[15] http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

infancy, it has important potential and offers many possibilities for use for security purposes.[16] Police in Orlando are using an experimental facial recognition program from Amazon. Thus, companies that supply body cameras for police officers can now add facial recognition software to them. The Axon company (formerly Taser) is responsible for manufacturing and supplying tasers and body cameras to police officers throughout the United States. The company expressed an interest in adding this application to the body cameras it provides to the police, which will allow the police to scan and identify faces while on patrol and, in principle, identify everyone they see.[17] As noted, this technology has tremendous potential in locating suspects. However, it also raises fundamental issues regarding the right to privacy and the appropriateness of protecting government databases; these issues justify an in-depth discussion that exceeds the scope of this report.

- Artificial intelligence can be harnessed for counter-terrorism purposes. One of the challenges of counter-terrorism is the fact that terrorist networks are composed of small cells of activists scattered around the world. This makes it difficult for security agencies to predict where a group is likely to strike next. The use of artificial intelligence and machine learning techniques has the potential to assist in mining vast amounts of information and in detecting discrepancies in suspicious situations.[18]

4.4. Legal Aspects

- The US Attorney believes that the most concerning security threat at the moment is cyber-terrorism, contrary to his previous opinion when he took office in the early 2000's. Cyber-

[16] https://www.forbes.com/sites/forbestechcouncil/2018/09/19/the-future-of-biometric-facial-recognition/#dcaac113c742

[17] https://www.youtube.com/watch?v=HGMLGnUrbKI

[18] https://www.leyton.com/blog/?p=1893-leveraging-ai-machine-learning-techniques-fight-terrorism

terrorism is an expression of activity that includes cybercrime syndicates, activities on the darknet, and "hacktivists" — individuals who promote a political agenda through hacking.[19]

- In June, a memorandum was published on the proposed Cyber Defense and National Cyber Directorate Law (June 25, 2018). The memorandum is intended to implement the government's decisions and policies in the field of cyber defense as well as the aspects related to the national cyber system and its powers. The memorandum stated that: "*In recent years there has been a significant increase in the frequency and severity of cyber threats. [Cyber] space has unique characteristics that facilitate the hostile activity within it: the short time constants that characterize the changing space and what happens there; the irrelevance of physical distance to activities in cyberspace, resulting in exposure to threats from around the world with similar probability; the relative anonymity that it affords; the absence of a security force to separate the attacker from the victim; the low cost of developing cyberspace capabilities; and an increase in the surface area for attack as a result of this arena's rapid expansion*".[20] According to the memorandum, the cyber system can regularly collect data from Internet and cellular providers, government ministries, local authorities and government companies in order to identify and prevent cyber-attacks in advance. The powers granted by the law to the cyber system raise concerns about civil right violations. Thus, the Israel Democracy Institute asks how necessary it is to store all the aforementioned information regarding our activities in cyberspace and whether there is concern that it will be used in the future to harm civilians. When there is so much information available to the state, there is a tangible threat to the right to privacy and other human rights.[21]

[19] http://www.wesa.fm/post/cyber-terrorism-and-domestic-extremism-among-greatest-terror-threats-us-attorney-says#stream/0 accessed 25.10.2018

[20] https://www.pc.co.il/featured/268980/

[21] https://www.idi.org.il/articles/23988

4.5. Publications of Official Documents and Opinions

- In September 2018, the White House published the US National Cyber Strategy, which details how the Trump administration will defend the homeland by protecting networks, systems, functions and information; promote the prosperity of the US economy by fostering a secure and innovative digital economy; maintain peace and security by strengthening the ability of the US and its allies to deter and punish users of cyber tools for malicious purposes, as needed.[22]

- In October 2018, the White House published the US National Strategy for Counter-Terrorism. In the document, it was stated that the American nation is still a nation at war. The terrorist landscape is more complex than ever before. Therefore, counter-terrorism continues to be a top priority for the Trump administration. The terrorist enemy is radical Islamic groups that seek to carry out global terrorist attacks, infiltrate the country's borders, and radicalize and recruit potential supporters within the US. The US continues to deal with threats from Iran, the most prominent terrorist-supporting state, through a global network of activists and a system of terrorist groups. Terrorists motivated by other forms of radicalization also use violence to threaten the homeland and American interests. These terrorist threats differ in many ways, but they all seek to use violence to undermine the US and interfere with the American way of life.[23]

- In the framework of this strategy, emphasis is placed on cutting off terrorists from sources of financial, material and logistical support. The technological progress of the last century has created a connected world in which it is easier than ever before to motivate people, and to transfer funding, material support and information around the world. The backbone of this linked system is information technology - much of which is the product of the US government and private US companies. The document notes that, in modern times, it is difficult to disrupt terrorist activity because terrorists adapt themselves to a changing environment and use many

[22] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[23] https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf

means to achieve their goal. In the US, they misuse technology, such as the Internet and encrypted communications protocols, to promote their malicious goals and spread their violent ideologies. The main tasks set by the US administration are: 1. To identify terrorists in key positions and terrorist groups through military and non-military means, including leaders, operation planners, and individuals who use their areas of expertise, such as weapons of mass destruction, explosives, cyber operations and propaganda; 2. To expand access to overseas areas; 3. To effectively use administrative detention as a counter-terrorism tool in accordance with international law applicable to armed conflicts; 4. To integrate intelligence sharing between federal, state, and local levels; 5. To enhance the impact of counter-terrorism operations through strategic communication aimed at refuting the terrorist narrative, discouraging potential terrorism supporters, and demonstrating that the effect of US counter-terrorism operations is not limited to direct actions only.

- In September 2018, Europol's Organized Threat Assessment was published. The report reviewed cyber-crime incidents, including ransomware attacks and online pedophilia. The report mentions the use of bitcoin for illegal activities on the Internet. In the past, groups affiliated with terrorist groups have called for donations via bitcoin, including Akhbar al-Muslimin, Dawat ai-Haqq, Isdarat, and more.[24] The report indicates that solicitation for bitcoin donations was made to finance the online infrastructure and to acquire host servers. However, one crypto-based campaign – a charity – appealed to Muslims in the West to enlist as fighters in the war in Syria. Despite the potential, none of the attacks that were carried out on European soil were financed by virtual currency, according to the report. The use of virtual currency by terrorist groups included only low-level transactions. Their main financing still comes from conventional banking and money transfer services. The report concludes with two ways to combat terrorism financing: First, to defeat the distributors of propaganda and recruitment through intelligence sharing

[24] https://www.ict.org.il/images/Jihadists%20Use%20of%20Virtual%20Currency.pdf

between law enforcement agencies. And second, to focus on their ability to carry out cyber-attacks.[25]

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.

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

[25] https://www.ccn.com/bitcoin-hasnt-funded-any-terror-attacks-in-europe-europol-report-reveals/ and https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018 both accessed 24.10.2018

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