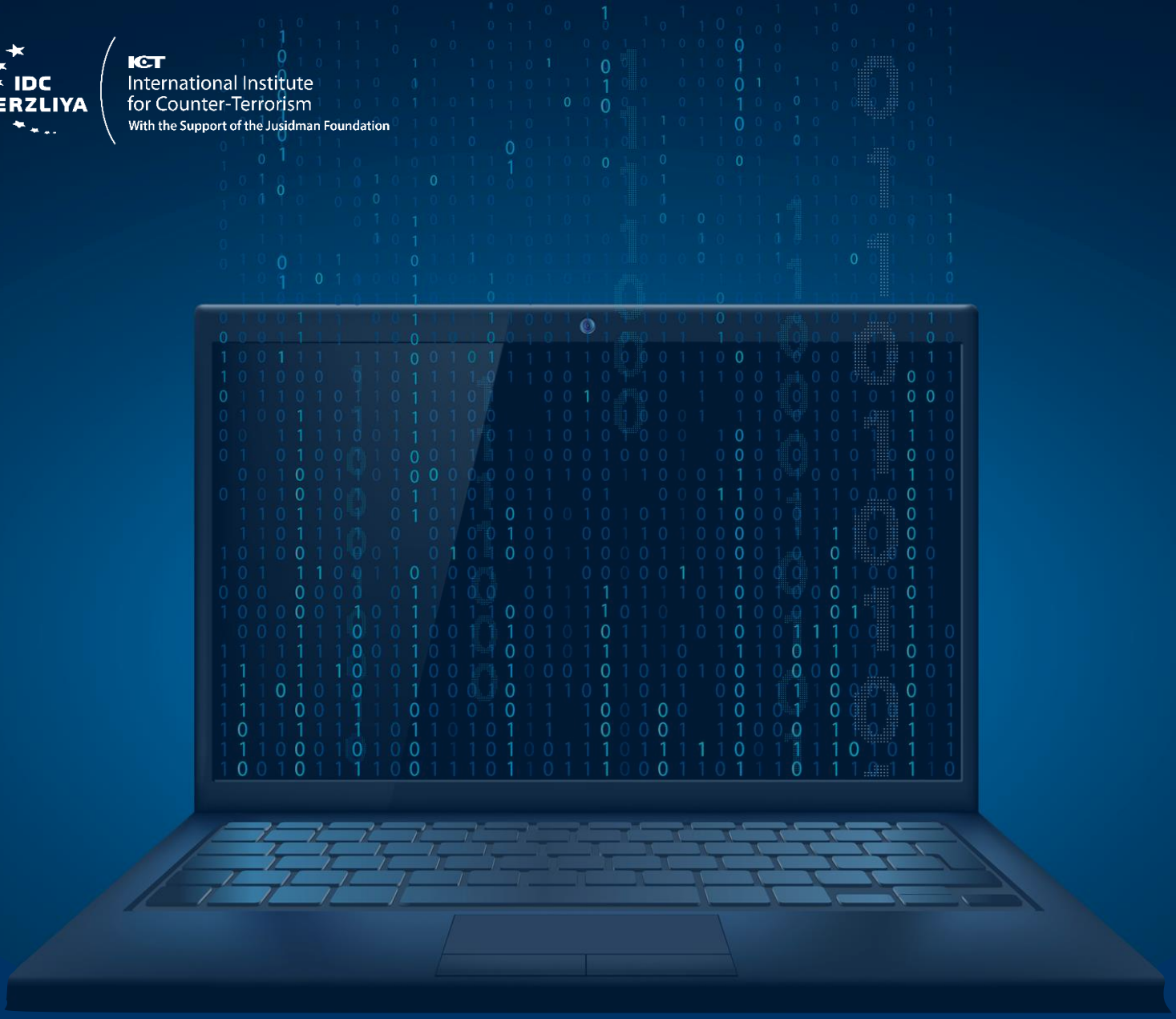
IDC HERZLIYA

ICT International Institute for Counter-Terrorism

With the Support of the Jusidman Foundation



Cyber Report

July-September

2019

Executive Summary

The potential of cyberspace has been identified by terror organizations over a decade ago however only in recent years one would have observed a significant increase in the scope and sophistication of use of the internet by terror elements. At first terror organizations only made use of web sites, later they have expanded those to include some interactive elements and to date, via social media networks and various applications, these organizations are fully interactive. Among terror organizations, **ISIS** is considered a trail blazer and an innovation leader in that respect. The traditional hierarchical structure that typified terror organization has been undergoing dynamic changes in recent years, including the deployment of command and control apparatus. Thus, next to the hierarchical organization structure prevalent in territories under the terror organization's control, a web-based apparatus has been forming in other territories and is enabled by the growing use and accessibility of the internet globally.

In the period between July and September 2019 terror activity in cyberspace has been identified in three major levels:

Operational – Jihadi organizations keep using cyberspace for a variety of uses. The most prominent are propaganda, recruitment, "lone wolf" activity encouragement and finance campaigns.

Defense – No major shift in the terror organizations' cyberspace defense concept has been observed. They keep disseminating content on data security and encryption, privacy and anonymity, warnings from imposters and instructions for secure use of mobile phones. Further, terror organizations continue their efforts to improve their offensive capabilities however those have not yet matured and still revolve around low level hacking of social media accounts and defacing websites.

Response to global counter cyber security efforts – a growing trend of using subcontractors to disrupt the operation of critical infrastructure has been identified. Hence, cyber security experts highly recommend implementing high security standard all along the critical infrastructure supply chain. Operational activity by law enforcement to shutdown web-based criminal and terror activity has kept going on and technology companies and governments promote collaborations to contend with inciting online materials.

Contents

Executive Summary 2

Operational 5

Propaganda 5

Recruitment 15

Finance 16

Defense 22

Offense 26

International Response 27

Government and Critical Infrastructure 27

Law, Policy and Regulatory Regime 28

Geopolitics and Terrorism 30

State Sponsored Hackers 31

Cyber Cooperation 32

Operational

Jihadi organizations make use of cyberspace for a variety of needs, the most prominent are propaganda, recruitment, "lone wolf" activity encouragement and finance campaigns as follows:

Propaganda

Even though **ISIS** has been backed into a strategic corner and loss of territories, it seems that as far as propaganda is concerned the organization keeps putting a lot of effort into preserving its ability to start new campaigns , recruitment and fund raising.

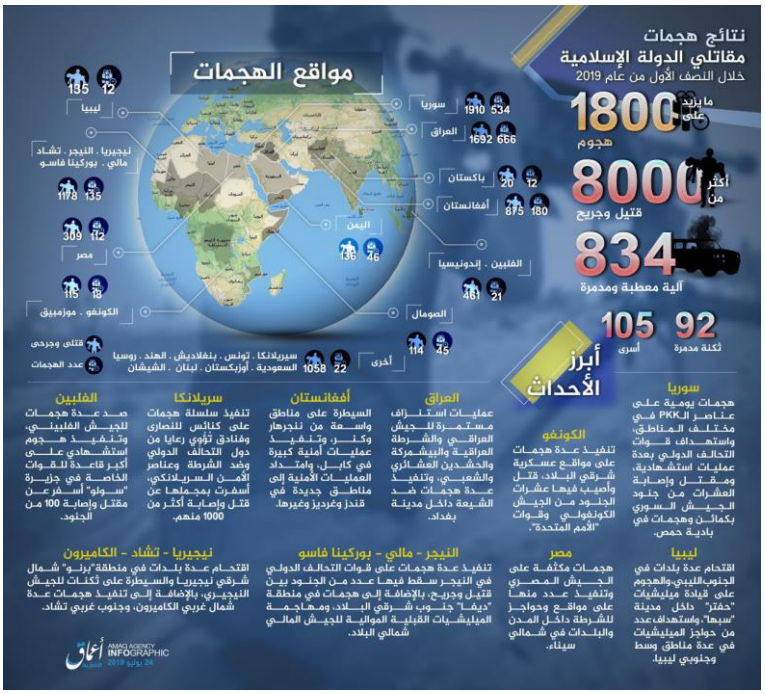
- **Al-Saqri for the Science of War** media outlet, assisting with **ISIS** propaganda posted the following:
  - An announcement (see photo) on opening an online Telegram class on "military medicine" for jihadists and whomever wishes to enlist (Telegram 17.8.2019)[1]. Similarly, they announced on the opening of an explosive and explosive devices class (Telegram 27.8.2019)[2].

[1] 17.8.19. Telegram.
[2] 27.8.19. Telegram.

- An old article on the importance of focusing on employment of electronic warfare against the enemy. Per the writer, one of the main reasons to the enemy's might is its technology and modern technological tools that enable it to conduct electronic warfare. In light of that the writer stressed that jihadists are required to study how to conduct electronic warfare as "it merges with the modern traditional war". The writer added that within the framework of electronic warfare the enemy seeks to achieve information on jihadists and spy on them, disrupt their communication, locate them,
- identify their capabilities and weaknesses, conduct psychological warfare by disseminating fake news and spreading rumors and more. Therefore, jihadists must become professionals in electronic warfare and move from defense to offense in the electronic arena. For example, deepen their knowledge and develop encrypted communication devices and raise awareness to fake applications intended to serve as spyware (Telegram 3.8.19)[3].
- In the first half of August 2019 **al-Sahab** media outlet, owned by **al-Qaeda**, posted vol. 2 of the magazine **al-Ummah al-Wahida**. One of the articles discussed the importance of weakening the U.S. economy and its allies via the internet by conducting hacking and cyber-attacks. The organization called jihad supporters to concentrate their efforts against critical infrastructure such as power and water systems to paralyze life in enemy countries (Telegram, 10.08.19)[4].
- **Amaq** agency, owned by **ISIS**, posted an infographic containing information on attacks carried out by the organization since the beginning of 2019. For example, it said that the

[3] 3.8.19 Telegram
[4] 10.8.19 Telegram

- organization carried out 1,800 attacks, killed and injured over 8,000 people and destroyed approx. 834 armored vehicles[5].



The Amaq Infographic

- An ISIS supporting web user mentioned that Telegram has over 10,000 users assisting with ISIS propaganda, while there is no real activity on Facebook or Twitter and this needs to be remedied. For that purpose, he provided a Telegram address for a group called “Katibat al-Ansar” that oversees generating Twitter accounts and disseminating them to ISIS supporters[6].
- ISIS supporters posted on social media a banner detailing the media outlets assisting with the translation of the organization’s propaganda to various languages. The above points to

[5] 24.7.19. https://pastethis.to/mam0kmOcmko9A
[6] 16.8.19 Telegram

- the organization's wished to expand its audience and therefore they approach target audiences in their native language. The existence of informal propaganda outlets points to ISIS' decentralization in an era of developing technology. The following are the media outlets mentioned in the banner[7]:
  - Halummu – English
  - Al-Nur – French
  - Meydan – Turkish
  - Darrssalam – Indonesian
  - Irshad – Russian
  - Al-Tamkin – Bengali
  - Dawlah al-Islamiyah Sharqu Asia – Philippines
  - Black Flags – Pashtu
  - Al-Hijrateyn – Swahili
  - Nadat Hak – Urdu
  - Ajnad al-Khilafa in India – Hindi
  - Rasta Re – Kurdish
  - Nahwand – Farsi

[7] 20.8.19 Telegram

The banner detailing translation groups for ISIS materials to native languages

- Vol. 11 of **Shabab al-Khilafa** posted details on software used by the organization's supporters to design and edit its propaganda, including Adobe Premiere, Adobe after Effects, Cinema 4D and Movvi Video Editor[8].

[8] August 2019 Telegram

- An informal media outlet called **al-Dar' al-Sunni**, assisting with **ISIS** propaganda, announced that it collated all of the organization's propaganda materials from 2016-2019 into one downloadable file. It said that the file contained over 1,000 propaganda items including video clips, audio clips, articles and more[9].

- An informal media outlet called "**Let's Storm"**, assisting with **ISIS** propaganda and focuses on disseminating its propaganda on Twitter, called its supporters to use its eservices as part of their assistance for the organization's propaganda. It said it had ready to use tweets that only need to be copied, pasted and disseminated; hacked Twitter accounts; phone numbers to validate Twitter accounts. Also, it provided a link enabling contact with it to join it.

[9] 13.9.2018 Telegram

Let's Storm tweet calling ISIS supporters to copy, paste and disseminate pre-made ISIS propaganda

- A Telegram channel titled "**The Attack Company**" assisting with **ISIS** propaganda, called the organization's supporters to use its eservices to disseminate the organization's propaganda on Twitter. In a banner posted on Telegram it said that it specialized in propaganda campaigns, hashtags, disseminating propaganda to smear the enemy, planting ISIS messages on Twitter, providing Twitter accounts to ISIS supporters and more.

- Upon the conclusion of the 1440 Muslim year (September 2018-Septemebr 2019), **al-Naba** (**ISIS**' formal publication) an infographic on ISIS activity during that year. for example, ISIS carried out 3,665 military activities that led to the death of 15,845 people. Iraq and Syria provinces are leading with the highest number of dead and injured (over 4,000 dead or wounded). In addition, details of the organization's tactics were provided. For example, 95 suicide attacks were reported for the above period[10].

Al-Naba infographic re Muslim year 1440

- **Muta** news agency, assisting with **ISIS** propaganda posted a cluster of photographs of the organization's supporters posted to social media and show these people's support for ISIS following al-Baghdadi's speech in the second half of September 2019[11].

[10] September 2019, Telegram.
[11] 16.9.19 Telegram

A cluster of photographs of the organization's supporters posted to social media and show these people's support for ISIS

- **Al-Naba,** published by **ISIS**, celebrated its 200th volume with an infographic summarizing its activity since 2014. For example, since its first issue it published 31 interviews, 3,500 news items, 432 articles, 65 shahid stories, 388 infographics, 189 op-eds and 45 investigative stories[12].

[12] 27.9.19 Telegram

- **Sheikh Abdallah al-Mohseini**, a prominent Salafi jihadist cleric in Idlib posted a fatwah prohibiting the use of photography apps that change the users features to either younger or older ones, animal face etc. per him, it changes the image of man as he was created by Allah[13].
- **Dalil al-Ansar** media outlet, assisting with **ISIS** propaganda announced that it stopped all operations a while ago hence one should beware of any post made in its name. They also warned of an Iranian Shiite Telegram account purporting to disseminate content on its behalf[14].

Dalil al-Ansar banner

[13] 17.7.19 Telegram
[14] 2.8.19 Telegram

- **Hayat Tahrir al-Sham**, an umbrella organization for several jihadi factions in Idlib conducted between July and September 2019 an online recruitment campaign titled “Perform Jihad Yourself”. Within the campaign it was written that the residents of northern Syria and Hama are called to fight the enemy with their own hands, defeat it and drive it away. Further, it was written that the campaign wished to encourage young people living in the liberated areas of northern Syria to join the ranks of jihadists and assist with the fighting. One of the banners posted to social media provided details on the campaign. For example, in the first week since the launch of the campaign more than 450 people enlisted, 60
- clerics committed to assist it, 106 mosques called upon their members to join the ranks of the fighters and more[15].

Online banners posted within “Perform Jihad Yourself”

[15] July-Sep 2019 Telegram.

Finance

The use of internet to fund terrorism increased during the reviewed period. Some of the campaigns call for posting and disseminating calls for funding and some campaigns call for funding via crypto currency. The following is a select list of such campaigns:

- **Sheikh Abd al-Razak al-Mahdi, Sheikh Abu Muhammad al-Sadiq, Sheikh Anas, Sheikh Muslih Al-Ulyani and Sheikh Abdulla al-Muhaysini**, clerics close with Hayat Tahrir al-Sham and other jihadi factions in Idlib launched an online campaign titled al-Khandaq ("The Trench") aimed at " protecting the Syrian revolution and fight the Russian evil campaign to take over Idlib that stands tall". Sheikh al-Mohseini clarified that the campaign has two major goals: (i) fortification of dangerous areas by excavating tunnels and trenches and front lines; (ii) recruiting as many residents as possible to defend the liberated areas under the slogan "today we are all mujahidin". He added that the campaign may be assisted by donations, dissemination of propaganda and the campaign on WhatsApp and other social media platforms and by providing photos of supporters with the caption "today we are all mujahidin". Per al-Mohseini signing up for the campaign will reinforce the mujahidin's defense deployment and will put fear in the Alawi and Russian hearts. He stressed that a victory for the mujahidin in Idlib is a victory for the entire Islamic nation not just the jihadists' in Idlib. Further, within the campaign al-Mohseini called upon Muslims in Syria, the Gulf states, Turkey and other countries to donate money for the campaign. Per him, any amount, however small, is important in assisting the jihadists' victory in Idlib. He added that whomever wishes to donate can contact him via WhatsApp or Telegram. In other correspondence he posted names of Muslim donors to the campaign (from Turkey, Gulf

- states, Egypt, Germany and more). In another correspondence he wrote that the cost of excavating a tunnel is $15,000 and time needed to excavate it if four hours. Moreover, within the above campaign the clerics called Idlib residents to enlist the popular militias and various jihad factions including al-Jabha al-Wataniyah, Hayat Tahrir al-Sham, Jaysh al-Izza, and operation centers such as al-Fath al-Mubin and Haridh al-Muminin. Per them, anyone who wishes to join is welcome to do so via a designated phone number.

The Trench Banners posted by al-Mohseini calling to donate between $100-1,000 which will be used to excavate tunnels and buy tools

- **The Haridh al-Muminin** operations center (a joint operations center for several jihadi factions in Syria, including **Huras al-Din**, the al-Qaeda extension in Syria) launched a campaign titled Jahizuna (Arm us"), calling Muslims to donate money via Telegram and WhatsApp[16]

[16] 13.7.19. https://bayaan.info/archives/3301

"Arm us" Campaign banners

- In August 2019 **Saraya al-Muqawma al-Shabyya**, close to **Hayat Tahrir al-Sham** an online fund raiser titled "arm a warrior for Allah". The campaign was to arm civilians who wish to assist jihadists in Idlib. The campaign posted a price list for the equipment that can be bought with the donations such as military uniform for $28 and more[17].

Arm a warrior for Allah" campaign banner

- Activists identified with **Hayat Tahrir al-Sham, Saraya al-Muqawma al-Shabiyya and The Trench campaign** posted an online campaign titled "Fortify From Afar" calling Muslim, especially those

[17] August 2019 Facebook

- in Idlib to donate money to fortify the front lines and prepare for battle to block the enemy forces of Assad and the Shiite militias. It said that 7,000 bags of sand have been prepared and there is a need for people to deploy them to the front lines to fortify them. The banners further said that the campaign has been launched two months earlier by via a network of volunteers in Idlib and at this stage it was decided to expand it to cyber-space. The campaign provided Telegram and WhatsApp accounts to contact the campaign managers[18].

- **Al-Nasser Salah al-Deen Brigades**, a Palestinian Salafi jihadist faction in Gaza, kept running its social media platform under the title “Maddid” that ha been active for over two years. Within the campaign the organizers said that the donations are intended to arm the fighters who prepare for a jihad against the Jews until the liberation of the al-Aqsa mosque and Palestine. One correspondence said that any Muslim outside Gaza may contribute between $50-$100 and Gazans are asked to donate 50-100 ILS[19].

18 August 2019. Facebook

19 July-August 2019 Telegram

One of Maddid's banners , illustrating the organization's fighters are ready for battle with the Jews on Israeli soil

- **Ansar Allah**, the Houthi militia in Yemen launched a social media campaign to raise donations for the "children of mujahidin stationed in battle zones" to provide them with school supplies. The campaign posted a bank account number and a mailing address for the donations.

- **Jaysh al-Ummah al-Salafi,** a Salafi jihadist organization in Gaza close with al-Qaeda, continued its campaign "arm a warrior". A banner posted within the campaign contained a bitcoin account number to wire the donations to[20].

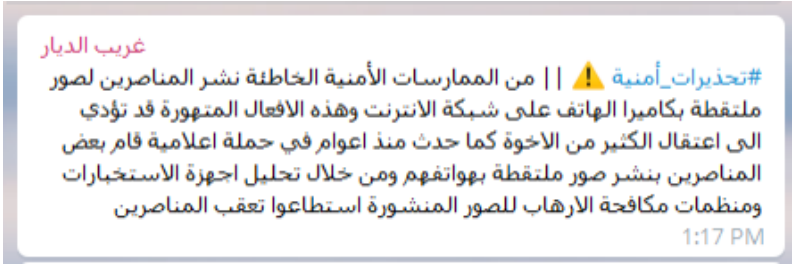
- Users of the jihadi forum **Shumukh al-Islam**, identified with **ISIS**, consulted on the safest way to finance jihadists on the front lines. Many users have responded that Bitcoin was a good way to do that however several others responded that Bitcoin was not so appealing as it loses its value, the trade is not 100% secure and the identity of the traders is identifiable. In Bitcoin's stead they suggested other crypto currencies such as Monero or Zcash. Another user mentioned that Bitcoin is a good option however it would be better to trade it on western exchanges because there are many places where it can be converted to USD[21].

[20] July-September 2019 Telegram
[21] July-August 2019. https://shamukh.net/forum/معسكر-الشموخ/3554734-تمويل-المجاهدين

Defense

Within the reviewed period no major innovation in the Defense strategy of terrorist online activity has been observed. The trend of continued dissemination of content on security and encryption, privacy and anonymity, warnings of impostors and instructions for a safe use of mobile devices. The following are examples of the above:

- A Telegram channel identified with ISIS warned ISIS activists of posting photos taken on mobile devices online. Per that channel such postings may lead to the arrest of many supporters, as has happened a few years ago when western intelligence and counterterrorism agencies managed to capture mobile devices and thanks to photos found on them were able to track and follow ISIS supporters[22]. Similar warning was posted in English: *"One of the wrong security practices of Ansar publishing pictures taken with their phone's camera on the Internet These actions may lead to arrest many brothers, as happened years ago, some brothers published photos taken from their cell phones, and by analyzing intelligence agencies and counter-terrorism organizations to these photos they were able to track the brother and arrested them"*



Warning of taking photos on mobile devices

[22] 17.9.19 Telegram

- In another correspondence ISIS supporters were warned of Telegram account posing as ISIS supporters' accounts containing erroneous advice on allegedly safe use of the internet. Per the correspondence, content and advice must be consumed only via formal Telegram channels[23].
- **Afaaq** media outlet, identified with ISIS:
  - An article on online payment method currently popular. Per them, the expansion of internet use and number of users and the upward trend of online payments necessitate knowledge of that subject matter. That said, they are aware that any material posted by a jihadi is monitored and analyzed by enemy intelligence and therefore the article will not provide exact and specific information but rather an executive summary of the current popular methods including, Western Union, PayPal, VISA/,AMEX/MASTERCARD, Bitcoin, Onecard, Paysafe. Further, the article warned the readers of transferring money in their own name claiming the transferor may be arrested by enemy intelligence and expose information that may endanger other supporters[24].

Banner for the secure financial conduct article

[23] 4.9.19 Telegram
[24] 9.7.19 Telegram

- A guide for maintaining safety while using Facebook. For example, the guide provided guidance on how to provide a fictitious phone number while opening a fake Facebook account that will serve as a propaganda dissemination platform; additionally, a recommendation to register to Facebook via a designated address provided by Facebook to Tor users[25].

- A guide on deleting metadata on Windows[26].
- A guide on deleting photographs metadata on Android[27].

- Telegram accounts identified with ISIS posted correspondence warning of the existence of interested parties posing as ISIS supporters and creating fake social media accounts to divide and sabotage the jihadi discourse. To contend with this threat ISIS supporters announced they will develop a platform called the Jihadi Fingerprint that will identify and authenticate ISIS supporters accounts. The developers described the system as having multiple stages of

[25] 29.8.19 Telegram
[26] 18.9.19. https://ehorizons.net/?p=309
[27] https://ehorizons.net/?p=161

authentication: in the first stage a person will be required to choose from five options regarding personal information on themselves. The information will be provided via response to questions that will have to be answered within a few days' time. for example, the questions will be on lessons or lectures ISIS prepared on the singularity of Allah, the reasons for the victories and defeats of the Israelites per the Islam, the separation of state a and church in Islam, the signs for Armageddon etc. once in receipt of the answers the platform will verify if indeed this was an authentic ISIS supporter account via an encrypted and secure social media platform. Once successfully crossed that barrier, the authenticated user will receive an identification number that will identify him as a bona fide supporter. The developers claimed that the Jihadi Fingerprint is not a formal ISIS initiative but rather that of a few supporters that pledged allegiance to al-Baghdadi and are committed to the resolutions and instructions of ISIS' propaganda bureau[28].

Banners for the Jihadi Fingerprint initiative

- **Al-Munasir al-Mutarjim** media outlet and a Telegram account titled Greenb1rds, assisting with ISIS propaganda warned users from Telegram spy who operated several suspect accounts that need to be blocked. Among the accounts mentioned:

[28] 18.8.19. https://justpaste.it/the_Islamic_State_

@Anis_54Almohads (682614353)

- Abu Furqan (758518150)

- @Anis_5Almohads (739128343)

- @Anis_1Almohads (637452063)[29]

Greenb1rds warning of the fake accounts

Offense

Terror organizations continued their efforts to improve their offensive capabilities however those are still at a low level and involve mainly breaking into social media accounts or defacing web sites. The following is a select list of the above:

[29] 10.8.19 Telegram

- The **al-Qaeda** leadership posted on vol. 2 of its **al-Ummah al-Wahida** magazine an article on the importance of developing hacking and cyberattack capabilities against critical infrastructure, water and electricity in particular, to paralyze life in enemy countries the U.S. especially[30]. Why this post is not on the hacking section?

International Response

Contending with cyberattacks requires global collaboration and out of the box thinking. The following are some steps taken by global actors to eradicate cyberattacks:

Government and Critical Infrastructure

- A report posted by the comptroller general of the U.S. Department of Defense (DoD), revealed that over 9,000 technology products, such as printers, cameras and computers, known to be susceptible to hacking and could be used to either cyberattacks or spying on military personal and sensitive installations were purchased by [31]DoD employees. Further, the report said that the Pentagon tended to buy equipment form companies such as Huawei, ZTE or Kaspersky even after government agencies identified them as posing threats to cyber security so much so that Congress prohibited any procurement from the. The report alerted that if DoD will continue to procure off the shelf technologies without identifying, assessing and preparing to counter any vulnerabilities in such technologies then missions critical to national security may be at risk (July 30th, 2019).
- The U.S. Army held a series of exercises in various cities in collaboration with the public and private sectors to promote municipal cyber security and response capabilities to cyberattacks. The series of exercises is called Jack Voltaic and is an initiative started by the institute for military

[30] 10.8.19 Telegram
[31] https://www.rollcall.com/news/policy/pentagon-dod-workers-bought-thousands-of-hackable-chinese-electronics-spy

cyber at West Point (ACI). At the core of the initiative lies the concept that upon the occurrence of a cyber attack on municipal infrastructure there may be a several days delay in the arrival of U.S. Army support. Therefore, the exercises were meant to reinforce independent municipal resiliency and empower local communities to defend themselves in case a massive cyberattack occurs. The first drill was held in New York, the second in Houston and the third is to be held in South Carolina and Georgia in February 2020 and will cover the region from Savannah (GA) to Charleston (SC). Furthermore, an exercise that will simulate the deployment of U.S. troops in Europe, called Defender 2020, is to be held as well (July 31st, 2019)[32].

Law, Policy and Regulatory Regime

- Many corporations in Australia are battling with massive legislation and regulations regulating privacy and cyber security. Michelle Price, a cyber security consultant warns that a large body of law create massive economic confusion and without clarifying the regulatory regime the Australian economy is likely to be harmed. In July 2019 the Australian Board of Consumers recommended a review of the Australian privacy laws as part of its review of new online trading platforms. Simultaneously, the Authority for Fair Commerce published new standards charging the entities under its regulatory jurisdiction to report any significant information security vulnerability which cannot be remedied promptly. Jennifer Stockwaell, a cyber consultant added that she hoped to see more regulatory coherency in terms of information security[33].

[32] https://www.c4isrnet.com/dod/army/2019/07/30/how-the-army-is-strengthening-cyber-cities/
[33] https://www.computerweekly.com/news/252467555/Australian-firms-grappling-with-train-smash-of-security-legislation

- More in Australia. The federal government announced their wished to change the Australian cyber security strategy, in place since 2016. Per the government the nature and level of threats to individuals and business has changed and requires an improvement in cyber security, especially since Australia wishes to stand at the forefront of global cyber security. To prepare the for the new strategy the government posted a preliminary document titled "Security Strategy: A Call for Views" which included 26 questions to the public. Some of the questions dealt with various cyber threats, the public needs and more. The deadline to submit answers was scheduled to November 1st, 2019 (September 6th, 2019)[34].
- The new Chinese cyber security suggestions may complicate the trade talks with the U.S. in recent months China published its suggestions along with several laws and standards aimed at curbing the transfer of certain data out of China. Additionally, it introduced stricter laws for equipment security. Should the suggestions be accepted, many American companies, over various sectors may be affected. This includes technology companies such as Dell, Cisco, Juniper, IBM as well as financial services and auto industries. Experts are of the opinion that the timing of the publication, which covers some eight categories was meant to show the U.S. that China has tools to penalize American companies as long as the talks carry on[35].
- U.S. congress passed two bills dealing with small business cyber threats. The first, requires the Small Business Administration (SBA) to inform any small business of cyber security incidents within 30 days (H.R. 2331 SBA Cyber Awareness Act)[36] and the second requires the SBA to start a certification program that will train 10% of its employees, in any of its centers, to provide information on cyber preparedness and assist and advise small business on ways to develop a

[34] https://www.zdnet.com/article/australia-is-getting-a-new-cybersecurity-strategy/?&web_view=true
[35] https://www.pymnts.com/news/security-and-risk/2019/chinas-cybersecurity-rules-us-trade-talks/
[36] https://www.congress.gov/bill/116th-congress/house-bill/2331/text

comprehensive cyber strategy for their businesses (H.R. 1649 Small Business Development Center Cyber Training Act of 2019) (July 29th, 2019)[37]. The above are meant to increase awareness for cyber threats among small business owners and assist them with developing their cyber strategies.[38]

- The U.N. has announced in September 2019 that 27 states have signed a commitment to encourage responsible cyber behavior, encouraging other states to join them. The commitment includes sections on a duty to implement and observe the implementation of international law regarding cyber space as well as understanding that the use of cyber space is beneficial however malicious behavior such as harming democracies and international organizations. Among the signatories are Australia, Canada, New Zealand, U.K., U.S., Italy, Poland and more (September 25th, 2019)[39].

Geopolitics and Terrorism

- A new report warns that cyber vulnerabilities connected to military systems, especially command and control one, have been examined by the Royal Institute for International Relations within NATO member states. The report titled "Cybersecurity of NATO's Space-Based Strategic Assets" said there was an immediate need to address such vulnerabilities of strategic assets within NATO and its member states, especially threats to satellite based command and control systems. The increasing vulnerabilities of satellites, ground stations, command and control systems and the teams running them have not received their due attention. There is an increasing need to embed military grade and specific cyber security capabilities to civilian products that may support military applications. If the above would not be addressed then items

[37] https://www.congress.gov/bill/116th-congress/house-bill/1649/text
[38] https://www.proofpoint.com/us/corporate-blog/post/congress-passes-two-small-business-administration-cybersecurity-threat-bills
[39] https://cyware.com/news/27-countries-pledge-to-promote-responsible-cyberspace-behavior-54a306e6

- procured from the civilian industries may have design flaws which will expose NATO systems to additional vulnerabilities (July 29th, 2019)[40].

State Sponsored Hackers

- State sponsored hacker groups monitor mobile devices for espionage, intelligence gathering and sabotage targets. Mobile malware is being developed by nation states to monitor separatists, journalists and others. Whereas the scope of such attacks is limited at the moment, a new research warns of mobile device focused state sponsored attacks. The transition to mobile device focused attacks stems in part from a growing adoption of computer protection and from the fact that users are more naïve as far as protecting their mobile devices, even though smart phones contain large amounts of personal information on users, who they interact with and so forth. The GPS in mobile devices enables pinpointing the user's exact location which may pose a physical risk to them. Thus, China, North Korean, India, Pakistan and other countries are notorious for disseminating mobile malware to monitor people either inside their territory or out. For example, in a North Korean campaign, regime dissidents were monitored via the installation of trojan malware mobile devices. The Syrian Electronic Army – sponsored by Bashar al-Assad – monitored dissidents via the installation of trojan horses in instant messaging platforms, including WhatsApp and Telegram[41].

[40] https://www.fifthdomain.com/international/2019/07/30/the-next-cybersecurity-concern-for-nato-space/
[41] https://www.zdnet.com/article/why-nation-state-hacking-groups-are-increasingly-turning-to-mobile-malware/

Cyber Cooperation

- The NSA announced the formation of a new cyber administration that will oversee foreign threats intelligence gathering and cyber protection. The new administration will be charged with preventing and reducing threats to national security and defense industries. It will be headed by Anne Neuberger who led the team that handled Russian threats within the NSA (July 24th, 2019)[42].
- The Indian Department of Telecommunications (DoT) plans to start a cyber academy to train government employees in the various ministries. That said, they also consider training officials from other countries to jointly fight cyber-crime. States that have already expressed interest in the venture are Qatar, Oman and Kuwait. The idea behind the academy is that the technological innovation encouraged by the prime minister will not be vulnerable due to lack of basic knowledge and awareness of government employees to the threats in cyberspace (July 22nd, 2019)[43].

[42] https://edition.cnn.com/2019/07/23/politics/nsa-cybersecurity-directorate/index.html?&web_view=true
[43] https://telecom.economictimes.indiatimes.com/news/india-to-set-up-cyber-academy-to-train-public-servants/70326375

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