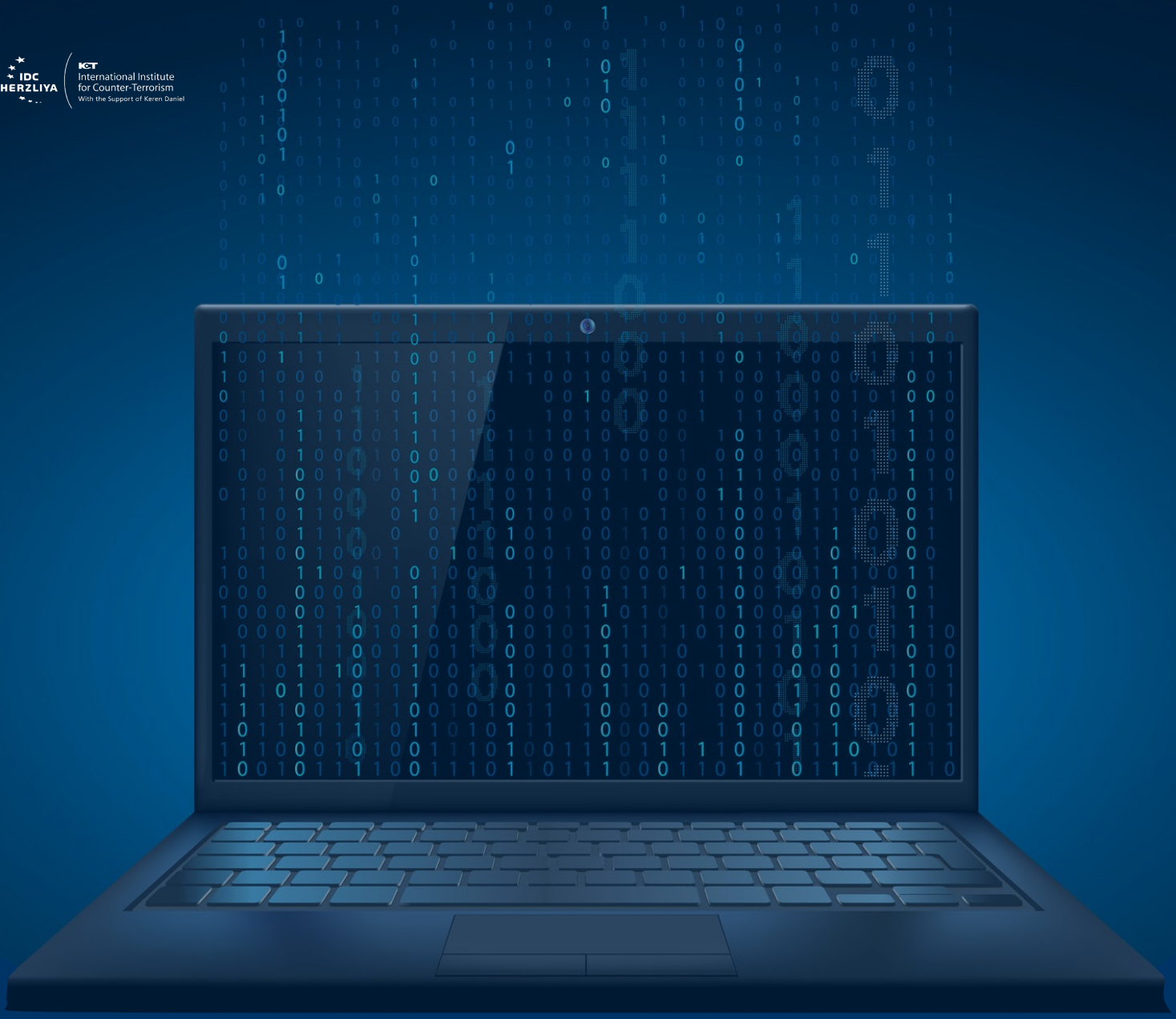
IDC HERZLIYA

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



Cyber Report #30

January – March 2019

Executive Summary

The potential of cyberspace has been identified by terror organizations over a decade ago however in recent years there is a significant increase in the scope of their use of cyberspace as well as with the level of sophistication of such use. At first, terror organizations used static web sites, then some interactive elements have been incorporated into them and to date with the prevalence of social media and various apps, terror organizations are fully interactive. On that note, as far as "cyber for terrorists" is concerned, ISIS is considered an innovative trail blazer.

The traditional hierarchal structure of a terror organization is undergoing changes in recent years. Thus, in light of the growing accessibility to the internet, alongside the traditional hierarchy in territories under the direct physical control (or reach) of the organization there is a web-based network in other territories.

Within the period covered by this report, terrorist activity has been identified in three main areas:

The operational-administrative area. This where most of the activity has been observed. It includes communications, propaganda, recruitment, Psy-ops, training, intelligence gathering, data share and finance. One of the major trends I this area is the increased use of growing number of platforms (social networks, apps, forums etc.) that are being used for the above and the more targeted message to the audience using each platform. Another growing trend is the use of virtual currency to fund terror.

The defensive area. This deals with information security and manuals for safe and anonymous use of the internet have been published by terror organizations.

The offensive area. The use of cyberspace here was intended to serve the operational-administrative area (e.g. defacing or disabling other web sites, hacking, publication of kill lists etc.). Terror organizations don't own independent cyber attack capabilities, YET, however these may be acquired online or provided by state actors. Even though, within the period covered by this report, the number of cyber-attacks by known hacker groups was relatively low, an upward trend for the recruitment of ISIS supporting hackers has been observed in South East Asia.

Table of Contents

1 Operations

1.1 Propaganda and Recruitment

Identifying the potential of the internet as a means to disseminate messages coupled with gaining expertise in high technology, software, web sites, social media, social networks etc. improve the effectiveness of a terror organization's propaganda. **The propaganda strategy of terror organizations has significantly evolved in the past decade**, due to two major processes. The first, the accelerated technology evolution that brought on **new online platforms** and the diverted traffic from web sites and forums to social media. The second, the emergence of new online actors, especially ISIS, **increased the use of cyberspace**. For example:

- ISIS supporters on social media uploaded banners warning Muslims from consuming content broadcasted on enemy controlled media outlets and sermons preached by Muslim clerics employed by corrupt Muslim regimes.

Left to Right: "The Sheikhs of Satellite Channels: Direct Broadcast"; "Paralysis of the Mind"

- A guide titled "Advice for the Invader" on how to disseminate propaganda on Twitter. For example, it recommended to tweet every two minutes and not immediately; similarly, limit hash tagging to three consecutive times to avoid having the account blocked by Twitter. Further, the guide recommending planting messages in accounts owned by clerics employed by the tyrannical regimes; retweet messages posted by ISIS supporters and so forth.

A post on Telegram on how to disseminate ISIS supporting messages on social media.

- Links for downloading a comprehensive archive with audio, video, transcripts etc. published by jihad leaders, including Osama Bin Laden, Abu Masab Al Zarqawi, Abu Bakr Al Baghdadi and more

Banner for the above-mentioned archive

- Some Syrian Salafists have mentioned that have reopened their Snap accounts after the former ones have been closed by the company

-

1.2 Financing

In January 2018 ICT published a review of the jihadist use of crypto currency. During Q1/2019 it seems that this use has picked up as follows:

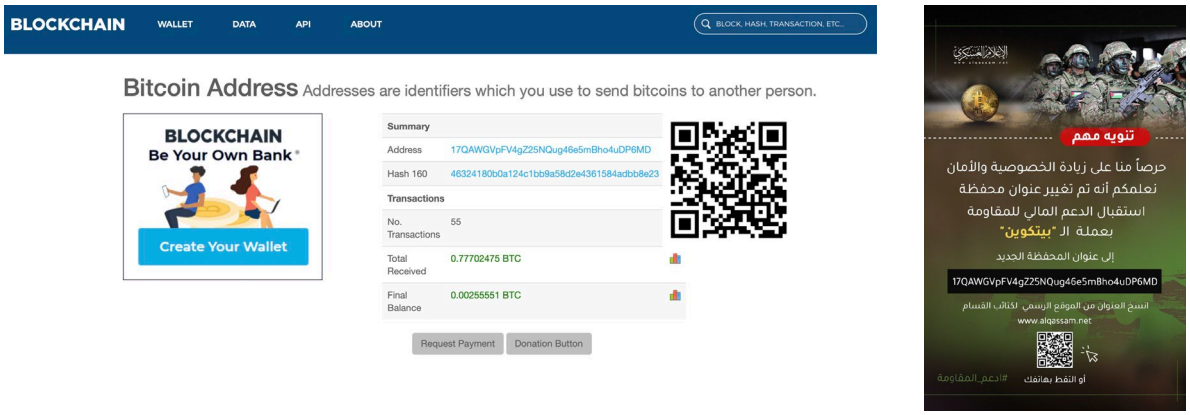
Hamas

On Hamas' Telegram channel ICT identified a campaign calling for donations for the organization via Bitcoin following the reduction of foreign aid (January 30, 2019). Within the campaign many banners were posted, calling for donations and referring to various virtual wallets

- Hamas' military arm launched towards the end of January an online campaign to raise funds via Bitcoin. Abu Ubeida, a Hamas spokesman, called Muslims to donate and mentioned that a detailed explanation on the donation process will be provided at a later stage. Hamas' news agency Shehab, also published a clip urging people to donate Bitcoin. A guide on how to donate in Bitcoin has indeed been posted and included a referral to SpectroCoin to facilitate the donation.

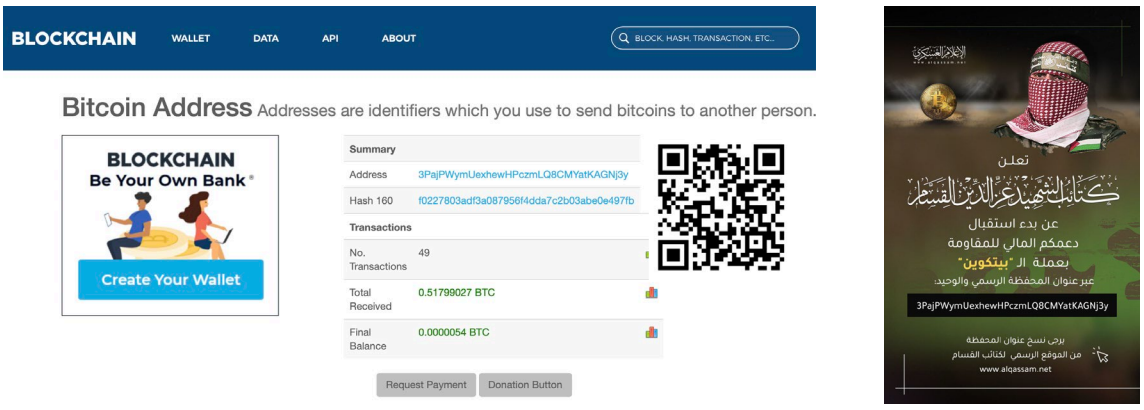
Telegram banners calling to donate to Hamas

- Bitcoin address 17QAWGVpFV4gZ25NQug46e5mBho4uDP6MD. Reviewing this address on Blockchain site revealed that between February 2nd, 2019 and March 24th, 2019 this wallet received 55 payments totaling 0.77702475 Bitcoin (approx. $3,095.5). most of the transfers were for low amounts ranging from a few US Dollars up to a few hundreds of Dollars.



Right: The Telegram banner with the bitcoin address; Left: The Hamas wallet on Blockchain web site

- Bitcoin address 3PajPWymUexhewHPczmLQ8CMYatKAGNj3y. Reviewing this address on Blockchain site revealed that between January 31st, 2019 and February 10th, 2019 this wallet received 49 payments totaling 0.51799027 Bitcoin (approx. $2,481.92). Similarly, the money transfers ranged from a few Dollars to several hundreds.



Right: The Telegram banner with the bitcoin address; Left: The Hamas wallet on Blockchain web site

- Moreover, Az Al Din Al Qassam web site has uploaded a clip containing details on the Bitcoin donation process and created a dedicated web site for that at https://fund.alqassam.net where they embedded **an algorithm that generates a unique address for every person wishing to donate** to

preserve their privacy and safety. This was not the first time terror organizations have used that type of algorithm. In January 2018 the web site Akhbar Al-Muslamin, that broadcasts ISIS news has activated a similar algorithm[1].

Right: A banner encouraging donation in Bitcoin; Left: A screen shot of a unique address generation; (Source: Hamas' web site)

Saladin

- Saladin Brigades, a Palestinian Islamic faction in Gaza posted on its Telegram channel a few posts calling for donations in Bitcoin as part of its campaign "assist the Gaza mujahedin". In one of the banners (see image below) it was said that Jihad activists need weapons and provided a Telegram address to make contact. Yet, the use of virtual currency remained mostly anecdotal.

[1] See "Jihadist Use of Virtual Currency", The International Institute for Counter-Terrorism (January 2018), http://www.ict.org.il/images/שימוש%20ג'יהאדיסטים%20במטבע%20וירטואלי.pdf

That said, from the campaigns conducted since 2017 such as Jahezuna, Al Sadaqa and ISIS (Akhbar Al-Muslamin) as well as other campaigns the trend seems to be in an upward trajectory. In that sense the new phenomenon of using algorithms that generate unique Bitcoin wallets should be addressed in depth as it disrupts some of the transparency associated with the use of Technology Distributed Ledgers and encumbers forensic accounting investigations.

2 Defense

Over the past two years public and political pressure has been mounting on the web giants (e.g. Facebook, Goggle, Microsoft) to increase monitoring of the content disseminated on their platforms. In light of this activity the terror organizations have been putting in an increasing effort to anonymize their web activity and secure accounts associated with them. One of these actions is a **systematic dissemination of manuals for information security and user anonymity**, both while using apps and the internet and while storing information on various devices (phones, servers, hard drives etc.).

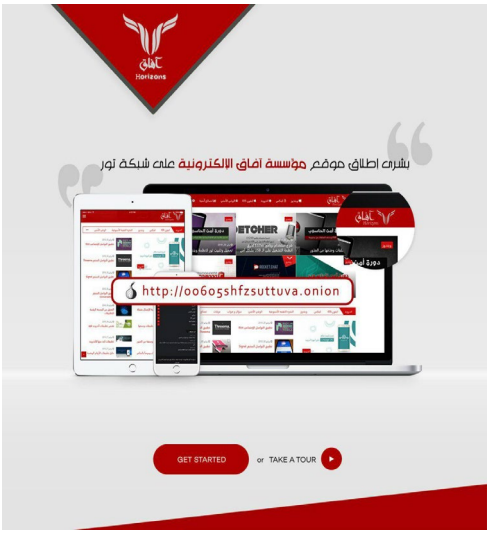
2.1 Defense Manuals

During January-March 2019, Afak media group, that is focused on increasing jihadi activists' awareness to online security, has posted tens of manuals on the subject, among them:

- A clip encouraging people to follow their activity on Tor
- A manual for the installation of Tor proxy on Telegram.

- News on updates in security and technology. Between January and March, the group published **volumes 21-33.** Of the news published on **vol. 21,** of note are the following: personal data collection and user monitoring by Facebook through various apps; successful jihadi hacks of Twitter accounts and planting jihadi messages on them; weather apps collecting user information; ransomware. Of the news published on **vol. 22,** of note are the following: Twitter can triangulate user location; Of the news published on **vol. 23,** of note are the following: security breaches on Twitter enabling reading private correspondence dating back five years. Of the news published on **vol. 24,** of note are the following: web sites can steal browser information through AP; cyber researches were able to shut down over 100,000 malicious web sites in ten months; GDPR fines Google Eur 50 million for violating regulations on transparency re collection of user information for targeted advertising. Of the news published on **vol. 25,** of note are the following: Facebook intends to encrypt Instagram messages. Of the news published on **vol. 26,** of note are the following: a virus affecting Linux has been uncovered; Google intends to provide a more sophisticated encryption for cell phones. Of the news published on **vol. 27,** of note are the following: Google warns of two security breaches on IOS.

- The group launched a dark web site. It was active between January and March and then stopped.



- ISIS has published on its formal weekly publication, Al-Naba (vol. 61), an article titled “The Importance of Encryption and a Warning from False Encryption”. The article stated that encryption of communications is of extreme importance because the enemy invests in monitoring jihadi activists’ communications. Yet, the writer warns not to fully trust messaging apps like WhatsApp, Skype and Telegram, claiming that despite developers claims, these apps have secret back doors in them allowing the developers to break in and monitor all communications. Moreover, today there are many monitoring means such as wiretapping via a device’s microphone, GPS tracking etc. Considering the above, the writer suggests verifying the credibility of the source offering a certain app prior to the installation to make sure it is not a monitoring app planted by the enemy. Alternatively, the writer suggests developing a jihadi encrypted messaging system, a possibility he claims scares the enemy.

- Hyat Tahrir Al-Sham, A jihadi Syrian Salafist organization, published in its magazine ABAA (vol. 36037) a two-part story on automatic installation of cookies on browsers, resulting in user personal data collection. Per the writer, to avoid this one better use Tor.

3 Offense

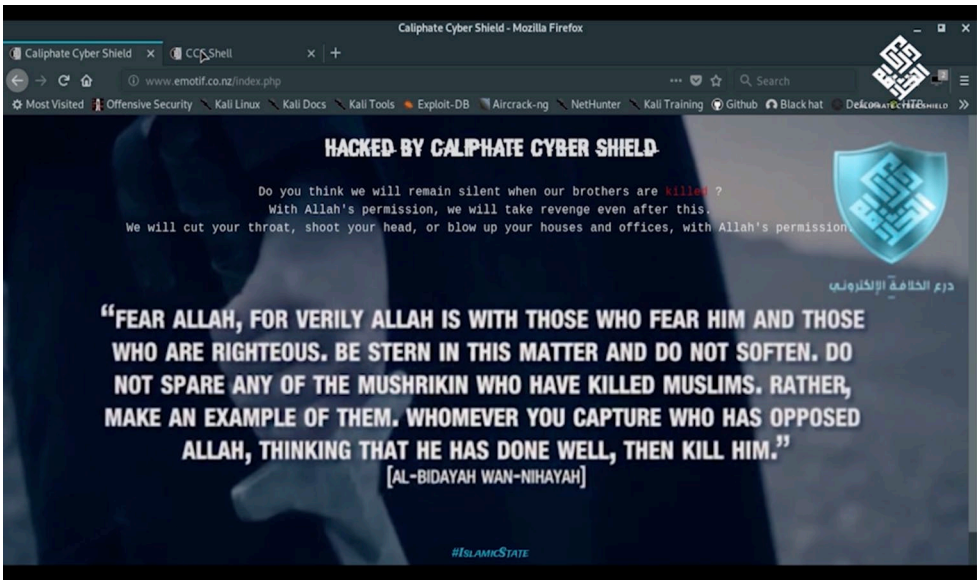
The nexus between virtual crime and global jihad is anecdotal however there is a growing trend of hackers joining the jihadi efforts in cyberspace. These are supported by the following findings in the time period covered by this report.

3.1 Cyber attacks

Caliphate Cyber Shield

On January 7th, 2019 a post on Telegram informed (in English and Arabic) of the formation of a new hacker group by the name of Caliphate Cyber Shield (CCS) as an offshoot of United Cyber Caliphate. The new group declared that it would start operating in the name of Allah and support of Islam and renewed its pledge of allegiance to Abu Bakr Al Baghdadi. The group It vowed to shut down web sites and hack infidels accounts.

- On March 15th, 2019 a mass shooting terror attack was perpetrated in two mosques in Christchurch, New Zealand. The terrorist, Brenton Tarrant (age 28) slaughtered Muslim worshipers and broadcasted his attack on Facebook Live. The attack claimed the lives of 49 people among them children. As a response, calls for revenge were disseminated online. For example, on May 1st, CCS posted a 27:30 minutes clip titled "revenge on New Zealand: out of your sites 2". It combines a collage of clips, some of which re military propaganda and some are cyber propaganda. One of the scenes shows a soldier shooting and immediately thereafter a screenshot of a hacker defacing a New Zealand web site. It seems that the author meant to equate kinetic fighting to a cyber one.



Clip: Revenge of New Zealand

- Another scene in this clip showed a prisoner of war being executed by ISIS when the photography is done from an FPS (First Person Shooter) point of view – which is an acceptable practice in video games. The caption "OH KUFFAR IN NEW ZEALAND" has been added in a bleeding red font to threaten New Zealanders. It is likely that the execution was videotaped by ISIS and not CCS but the addition of the point of view along with the video game theme suggests that the editor of the clip is a likely a teenager.

Revenge of New Zealand

- Additionally, Telegram showed a posting of defacing attacks perpetrated by CCS as a revenge for the Christchurch massacre. The sites defaced were of commercial companies and one university: http://ansaluniversity.edu.in/admin-assets/pdf/ ; https://wapa.asn.au/assets/uploads/ ; http://www.base.pro.br/source/index.html ; http://www.patro-tavier.be/source/index.html ; http://elrn.au-plovdiv.bg/uploads/manager ;http://www.commune-preuilly.fr/fr/images ; http://starnews.ge/public/source ;https://www.madridemprende.es/images/public/source ; http://www.arredamentirubinato.it/media/index.html ; http://www.nordnetimmobiliare.it/joomla/media/index.html. These were accompanied by **#RevengeNewZealand, #IslamicState, #OpTheWorld**.

- Contrary to the assessment that the fall of the physical Khalifate will increase the online activity of ISIS supporters, it seems that its main hackers' group – UCC- has disbanded. In its stead CCS was formed and it maintains similar characteristics. Seems like CCS is comprised of a group of teenagers with low technological capabilities that were driven by a sense of revenge on the Christchurch attack that will subside over time.

4 International Counteraction

Many countries came to realize in recent years that there is a real need to for a unique legislation in order to deal with cyber threats, terror related cyber threats included. Moreover, it becomes clearer and clearer that cyberspace does not leave a lot of room for each country's counter terrorism agencies to independently contend with such threats due to lack of physical borders and the rapid pace of technological advancement. In the period covered by the report the following legislation activity has been identified:

4.1 Law, Policy and Regulation

- A bill (The Senate Cybersecurity Protection Act 890) was introduced in the U.S., aiming to protect senators and their aides' immediate assistance in case their devices would be cyber attacked by state sponsored hackers. The bill was endorsed by cyber experts and elections activists (March 28th, 2019)[2].
- After the release of data showing that the U.S. Healthcare sector lost $6.2 billion in 2016 due to various hacking and data breaches, a healthcare industry specific data security document has been published aimed at protecting patient information. The document offers voluntary guidelines for organizations active in the sector and sets new standards in the field[3].
- China posted new regulations allowing the police to collect and verify electronic information in all forms and submit it as evidence in court. This move will also enable the police to freeze user web accounts. The Chinese Cyber Space Administration, de facto the Chinese cyber police, started to act against web sites and apps disseminating "negative information" (January 4th, 2019)[4].
- Calls for the U.S. to respect Chinese cyber sovereignty. Foreign technology companies storing information in China comply with Chinese cyber laws aimed to protect Chinese network integrity. The U.S demanded that China would stop discriminating cloud services suppliers (March 25th, 2019)[5].
- A bill was posted in NJ aimed at increasing reporting duties applicable to companies in case of personal identifiable information (PII). The bill aims to protect consumers from possible identity theft and help them to rapidly change account details in case breach happens. Should the bill pass it will reinforce the sense of privacy and security. It should be noted that the bill is only one of a few legislation initiatives introduced in NJ to arrive at similar regulatory regime as the one under GDPR in force since May 2018 (March 22nd, 2019)[6].

[2] https://www.bleepingcomputer.com/news/security/new-bill-to-protect-us-senate-personal-devices-accounts-from-hackers/
[3] https://www.natlawreview.com/article/healthcare-industry-reminded-to-heed-cybersecurity-new-industry-standard-guidance
[4] https://www.scmp.com/news/china/article/2180610/chinese-police-get-more-powers-collecting-electronic-data-evidence
[5] http://www.globaltimes.cn/content/1143392.shtml
[6] https://www.scmagazine.com/home/security-news/new-jersey-bill-would-broaden-pii-requiring-breach-notification/

- On March 12th, Utah legislators unanimously voted to pass a unique legislation supporting a new privacy law to protect electronic information stored by a third party (e.g. Google, Facebook) from access by the government. The law requires that law enforcement agencies need a court warrant if the want to access the information. On the federal level and every state but Utah, law enforcement agencies can access such information freely without any liability standards. In the U.S. there is a doctrine called "third party doctrine" set by the supreme court and stipulates that people cannot expect privacy on information they share with a third party. What that means is that the government has free access to any and all such information and the only barrier would the be the level of willingness to cooperate with the government of the technology company[7].
- The U.S National Institute of Standards published guidelines for companies on the protection of cell phones. It a guide on how to secure mobile devices with commercially available technology and was written together with tech organizations, government agencies and academia. The guide is a practical manual for creating network environment that will enable easy access to employees while reducing cyber threats. The guide also reviews several security solutions that meet NIST standards (March 19th, 2019).[8]
- A survey conducted among 500 information security experts, over 70% of the participants responded that they thought that states should have hack-back rights and over 50% thought that even private organizations should have that right and alternatively the right to retaliate in order to deter cyber criminals. Corporations and institutions are constantly under cyber attacks by either common cyber criminals (i.e. ones with just an economic interest driving them) and state sponsored ones. In case of defense contractors or organization with some government affiliation, state sponsored hackers are targeting sensitive technologies under development (March 19, 2019)[9].
- An Article written by law scholars and published on The World Economic Forum argued that the international law cannot keep up with the pace of the development of cyber attacks and cannot offer effective remedies. Further, the main problem with a cyber-attack is its designation: for a certain state actor to be held as responsible for a cyber-attack under the international law the attack has to be attributed to that state actor. However, when it comes to cyber attacks the state sponsored attacks are not official agent of the state actor but rather non state proxies that provide the state actor with a deniability. In fact, the problem is twofold. First, factually it is difficult to positively identify the culpable state actor with a high degree of certainty due to the borderless nature of cyberspace and its anonymity. Second, the International law does not recognize state actor liability to non-state actors' actions and therefore no liability may be assigned to state actor whose non-state proxies perpetrated cyber-attacks. Thus, the importance of investing in cyber defenses increases. (February 2nd, 2019)[10].

[7] https://www.wired.com/story/utah-digital-privacy-legislation/
[8] https://www.natlawreview.com/article/nist-publishes-guide-to-secure-organization-s-mobile-devices
[9] https://www.cbronline.com/news/cybersecurity-professions-hack-back
[10] https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks

- A bill was introduced in the U.S aiming at setting standards for IoT devices sold to the U.S. government. The bills call for contractors and other suppliers to comply with government directives in order to set an information security standard. In its current form the bill refrains from specific recommendations and calls for NIST to develop the standard. The goal is that such legislation if entered into law will bring about a more secure IoT equipment and trickle down form the government to the private sector and consumers in general (March 18th, 2019)[11].

4.2 Government, Military and Critical Infrastructure

- The U.S. military has been adopting a systematic method that takes into account that there are different levels of threats for information security. For example, the risk emanating from a device connected to the internet is higher than one who is not. Hence the focus is mainly on securing internet-connected devices. Another method being considered is avoidance, i.e. weighing whether connecting a certain device to the internet would be more an advantage than a weakness (e.g. connecting a tank component to the internet might be beneficial but not crucial and therefore the risk would be too high – March 29th, 2019)[12].
- Australia claims to be a world leader in cyber warfare (March 27th, 2019)[13].
- A survey conducted by Tripwire among cyber security experts revealed that two thirds of the experts had to change the location of their businesses and their business partners due to global cyber security considerations stemming from geopolitical issues. The geopolitical backdrop is also applicable to cross border cyber-attacks. For example, there have been attacks against U.S. energy infrastructure, NotPetya, Sony and WannaCry all of which have been attributed to state actors. On a similar note, the U.S. has banned the use of Kaspersky products in light of the concern regarding their involvement with attempts to unduly influence the elections (March 26th, 2019)[14].
- Senior officials said (at the information security convention of the Federal Resource Management Society) that protection of critical infrastructure in the U.S. require a paradigm shift towards cooperation between the public and private sectors. The panelists agreed that enhancing communication and cooperation are important today more than ever to secure critical infrastructure because the geopolitical threat facing the world today is nothing we have ever seen. The challenge exists on all fronts: land, sea, air and cyberspace and the main adversaries are Russia, China, North Korea and Iran (March 22nd, 2019)[15].

[11] ttps://www.darkreading.com/iot/new-iot-security-bill-third-times-the-charm/d/d-id/1334190?_mc=sm_iwfs_editor_kellysheridan
[12] https://www.afcea.org/content/army-takes-broad-view-cybersecurity
[13] https://www.afcea.org/content/army-takes-broad-view-cybersecurity
[14] https://www.computerweekly.com/news/252460164/Geopolitical-issues-affecting-cyber-security
[15] https://www.nextgov.com/cybersecurity/2019/03/defending-americas-critical-infrastructure-will-take-whole-nation/155755/

- Homeland Security invested $5.9 million in tools for cyber training for the energy sector. In fact , this was an expansion of a project that started with the financial sector. The training will include an interactive cyber training platform based on simulations and exercises aimed to address attacks on critical energy infrastructures and will allow the trainees to exercise and experience disasters in an online environment before they happen in the real world (March 25th, 2019)[16].
- Recently declassified DOD budget documents provide a glimpse into the equipment and training of cyber warriors and sheds light on the two most well-known programs of the U.S. Cyber Command: The Unified Platform and Persistent Cyber Training. In the past they worked separately however in light of the characteristics of cyber operations the DOD decided to unify both platforms into the Joint Cyber Warfighting Architecture platform that will provide the infrastructure for mission planning, data analysis and decision process (March 20th, 2019)[17].
- Brunei announced the formation of a national center for cyber security to defend the country from cyber threats. The center has been formed pursuant to the government's strategy to harness technology for economic benefits. Per Brunei, the formation of the center will allow the state to monitor and coordinate efforts on the national level to contend with cyber threats (March 20th, 2019)[18].
- North Korea perpetrated a cyber attack against critical infrastructure in various countries around the world. It started in October 2018 and intended to penetrate corporations in the following sectors: defense, finance, energy, communications, healthcare. It seems that the attackers using a phishing approach were able to penetrate some eighty-seven critical systems most of them in the U.S (March 14th, 2019)[19]. Following the attack, the U.S. issued a warning from North Korean cyber-crime and promised a forceful response. Homeland Security Secretary, Kirsten Nielsen, mentioned that in the past two years the world suffered the WannaCry attack that spread to 150 countries and held healthcare systems hostage for ransom. She added that on her threat list the word cyber gets a special attention (March 20th, 2019)[20].
- The Trump administration published a budgetary outline for a $9.6 billion for cyber defense for 2020, an increase of $1 billion from the previous year (March 14th, 2019)[21]. Further, it was announced that Homeland Security wished to hire some 150 cyber security experts through December 2020 at a cost of $11.4 million (March 18th, 2019)[22].
- European security agencies are preparing for a cross border large scale cyber-attack. In 2017, the WannaCry and NotPetya attacks stressed the lack of capabilities to contend with cyber-crime of that type

[16] https://www.nextgov.com/cybersecurity/2019/03/dhs-invests-59-million-cyber-training-tool-energy-sector/155808/
[17] https://www.c4isrnet.com/dod/2019/03/20/heres-how-dod-will-invest-in-the-cyber-mission/
[18] http://www.xinhuanet.com/english/2019-03/20/c_137910720.htm
[19] https://thediplomat.com/2019/03/north-korea-is-still-trying-to-hack-us-critical-infrastructure/
[20] http://english.chosun.com/site/data/html_dir/2019/03/20/2019032001460.html
[21] https://www.nextgov.com/cybersecurity/2019/03/what-dod-plans-do-96-billion-cyber-funding/155564/
[22] https://www.nextgov.com/cybersecurity/2019/03/what-dod-plans-do-96-billion-cyber-funding/155564/

and magnitude. To prepare for similar attacks the EU has adopted a law enforcement emergency response protocol. The protocol assigns a central role to Europol's cyber center (EC3) and is part of the EUI plan for cross border large scale cyber incidents. The protocol is a tool intended to provide support for European law enforcement agencies through immediate threat assessment, secure critical information sharing and effective coordination of cross border aspects of investigations (March 18th, 2019)[23].

[23] https://www.europol.europa.eu/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks

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