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

ICT Cyber-Desk

PERIODIC REVIEW

Cyber-Terrorism Activities

Report No. 17

April - June 2016

Contents

Highlights

This report covers the period of April-June 2016, with the following main issues:

- Terrorist organizations continued to perfect their online activities, and emphasized the use of various social platforms for distributing messages and directing to multiple websites. In this context, new accounts were opened on social platforms, and messages are posted as well as links to sites containing additional messages, especially on the dark net.
- The discourse among Al-Qaeda jihadists focused on the pros and cons of transferring their activities from forums to social media.
- In the field of cyber-defense, terrorist organizations are aware of the information gathering and preventative efforts by security agencies and therefore continued distributing defensive guidelines and moved to the darknet, where they claim to be better able to protect the traffic and anonymity of the organizations and their supporters, from tracking software of intelligence agencies, social networks and activists, who operate against terrorist organizations on the Internet in general, and on social networks in particular.
- Terrorist organizations continued their efforts to improve their offensive capabilities, but at this stage do not reveal significant technological abilities in this area. Nevertheless, it should be taken into account that these organizations can hire external bodies, such as those who identify with terrorist ideas or organized crime, and can also acquire such abilities from terror-supporting states. In this framework, it is worth mentioning a video published by hackers identified with ISIS, in which they claimed to have hacked into Twitter and Facebook accounts, where they posted a threat to attack the founders of Facebook and Twitter, if they continue to remove ISIS-related content and accounts. In addition, elements with ties to Al-Qaeda published details about security vulnerabilities of the Windows operating system while running remote applications.
- Counter-actions aimed at preventing the use of the Internet by terrorists continued, including the filing of civil lawsuits against owners of Internet platforms, such as

Facebook and Twitter. In addition, Microsoft expressed its willingness to cooperate in the removal of inappropriate terrorism-related content.

- The solid wall of money transfer services was breached in April 2016, when the SWIFT network, which acts as a crossroads for money transfers through messages, was fraudulently used to withdraw approximately 81 million dollars from the Central Bank of Bangladesh.

Introduction

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

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

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

Operational Usage by Jihadist Organizations

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

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

Jihadist Propaganda

During the period under review, jihadist organizations continued to carry out propaganda activities with familiar features from the past. Among all the activities worth noting:

- The launch of a Telegram account called "Official Applications", which includes links to ISIS-related applications and publications, such as a link to publications distributed by the organization during the month of Ramadan that can be downloaded via torrent file sharing software using peer-to-peer (P2P) technology. It should be noted that Telegram accounts are widely distributed and encrypted, and as such they are used as a convenient base to divert a target audience to applications and publications on the darknet.

The logo for the Telegram account, "Official Applications"

- The publication of an application for learning the Arabic alphabet, accompanied by militant photos aimed at children, for use on Android-based cellular devices and PC computers. The publication was carried out by the ISIS's printing house, Maktabat al-Himma, which is involved in the publication of links and applications. [2] It is worth nothing the ISIS's focus on children as a target population that it is trying to train for the future.

[2] 29.5.16. https://justpaste.it/uqi6

A banner for the application for learning the Arabic alphabet

- An appeal to the online public versed in Arabic to help with the transcription and linguistic proof-reading of jihadist publications. The appeal was made on the Twitter account of Al-Tahaya jihadist media institution, which is involved in publicity for Al-Qaeda. [3] It seems that the organization's intention was to improve the quality of its publications and to expand their distribution by focusing on recruiting people with knowledge in this field.
- Jaysh al-Sunna, a Salafi-jihadist faction belonging to the Jaysh al-Fatah umbrella organization that operates in Syria, invited visitors to join the WhatsApp group in the framework of which reports are distributed regarding events in the battlefields in Syria.

A banner providing the contact details of the organization via WhatsApp

- A new media group called Al-Iman, which supports the IS, published a new magazine titled, *Tawasul*, which focuses on – among other things – the importance of using social networks for publicity purposes, Islam's historical battles against Christianity

[3] 6.5.16. https://twitter.com/tayaha8/status/728632204327268353

and the organization's achievements in arenas of jihad. [4]

From left to right: details about the online PR campaign waged by supporters of the organization in praise of stabbing Jews; the banner page of *Tawasul* magazine

- Shortly after the terrorist attack in Orlando, which was carried out in June 2016 by an IS supporter, a Telegram channel called "Orlando Channel – Omar Mateen" was launched, which included publications encouraging Muslims in the west to carry out lone wolf attacks. One of the publications on the channel allowed visitors to download a computer program that contains videos, as well as official and semi-official articles by the IS and its supporters, regarding the massacre in Orlando. [5]

A screenshot of the software

[4] 3.5.16.
https://ia601504.us.archive.org/3/items/mterteing_tutanota_1_201605/%D8%AA%D9%88%D8%A7%D8%B5%D9%84%20-%201.pdf

[5] For further information, see: JWMG Desk, "Today in Florida, Tomorrow Berlin": The Threat by Islamic State Operatives to Attack Germany", *ICT*, 10.7.16. https://www.ict.org.il/Article/1731/today-in-florida-tomorrow-berlin

- On June 26, 2016 jihadists in Syria launched a "bot" on Telegram titled, "Mujahideen Bot", designed to spread information and guidebooks on military topics using bots and to encourage visitors to share information on the subject.

A screenshot from Telegram

Discourse Regarding Forums versus Social Networks

The shift from the use of Web forums to social networks, and the pros and cons involved, was widely emphasized in the jihadist discourse over recent months. The discourse covered the contribution of forums and social networks as central channels of communication, and the difference between the distributions of official publications and discussions held by the organization's supporters.

The following were the main points of the discourse:

- A visitor to Al-Fida jihadist Web forum, which serves as a platform for the official announcements of Al-Qaeda and its various branches, addressed the need to distribute an updated link to the forum that was removed from the Google search engine. The visitor randomly managed to find an updated link to the forum using the Twitter hashtag #شبكة_الفداء_الإسلامية. According to him, visitors must be made aware

that the forum continues to be active and, therefore, the new link should be distributed in every possible place on the Internet.[6] Another visitor noted that a link to the forum can be found on the tweet lists of senior jihadist leaders.[7]

- Fajr, a visitor to Al-Fida jihadist Web forum, which is affiliated with Al-Qaeda, claimed that jihad supporters used to publish official jihadist publications on various jihadist forums, but that today Al-Fida serves as the sole forum for the organization's official publications after various other forums, including Al-Hisba and Al-Firadus, were closed, and after the Shumukh al-Islam forum did an about-face and swore allegiance to the ISIS (after its director and his deputy were arrested). The visitor asked if jihadist forums had died out and if their supporters had ended their roles in the forums, and he emphasized that social networks are only partially to blame for the fading of the forums. The visitor asked the online public to speculate about the reasons for this trend.

  In response to this question, one of the supervisors of Al-Fida forum, known as Umm 'Amara al-Ansariyya, noted that social networks significantly contribute to this trend but, despite this, the forums remain an important action base and still deserve a place of respect. He added that all members of the forum, including the supervisors themselves, must concentrate efforts on increasing the discourse, creating topics for discussion and attracting outside readers. In response, Fajr remarked that it would be best to consider establishing a social network that would serve as an attractive platform for managing discourse and for sparking discussion among the youth. He emphasized that the forums used to be very strong in the area of propaganda but their time has expired, and he added that they must adopt the platforms used by the youth in order to strengthen the connection with them and to avoid falling into the trap set for them by intelligence agencies or enemies of jihad. In addition, he emphasized the need to think carefully and seriously about the issue of developing this action immediately.

  Another visitor responded and noted several factors related to the fading of the

[6] 21.6.16. https://al-fidaa1.net/vb/showthread.php?t=116457
[7] 24.6.16. https://al-fidaa1.net/vb/

forums and the rise in popularity of social networks, including the move of prominent writers from the forums to social networks and, with them, the public who used to consume their publications religiously. In addition, social networks allow the user to freely express opinions on social networks while the forums have a monitoring system over the content, which excludes content that it is inconsistent with the forum's management. The visitor claimed that official jihadist media institutions no longer need a mediator in the form of a jihadist Web forum in order to publish their jihadist materials (speeches, videos, etc.), but rather they can distribute them directly on social networks. According to him, jihadist forums have lost their uniqueness in the exclusive distribution of jihadist publications, which are being published today on social networks even before they are published on the forums. In addition, jihadist forums are characterized by uniformity and boredom such that, for the most part, they do not contain anything new, as opposed to social networks, which are characterized by relative innovation (the visitor did not specify in what manner). In addition, the visitor noted that jihadist Web forums serve the sole purpose of meeting archival needs by preserving Websites and information in case jihadist content is erased on Twitter and justpaste. The forums enable quick and easy access to content that was erased.

Another visitor noted that he agrees with most of what was said, but he emphasized that forums continue to maintain their uniqueness since the correspondence published on them originates solely from jihad supporters, in contrast to social networks where one can find a collection of jihadist publications from any source. He also emphasized that jihadist forums, especially Al-Fida, are still the source for official announcements by the mujahideen, and added that the lack of participation by several forum members was likely tied to security reasons. [8]

- A writer calling himself Al-Manjaniq ("the Catapult") wrote an article about the jihadist Web forum, Shumukh al-Islam. In the framework of the article, the writer claimed that the shutdown of the veteran forum was not accidental, but rather was a

[8] 23.6.16. https://al-fidaa1.net/vb/showthread.php?t=116461

planned move aimed at causing the organization's supporters to get lost "in the maze of accounts on social networks" and encounter false news items disseminated by opponents of the IS (it is worth noting that part of the US Army's offensive actions include the publication of false messages on the Internet – more on this later). In contrast to social networks, jihadist Web forums like Shumukh al-Islam allows access to authorized and reliable information but also serve as an archive for old reports and articles, which is not possible on social networks like Twitter where new accounts are frequently closed. The writer concluded by noting that activities on social networks should not be abandoned but, at the same time, jihadist Web forums should be supported and viewed as an "action base" or a platform for the continued delivery of jihadist messages.[9]

- A writer calling himself "Tenacious Supporter" published an article regarding the psychological battle being waged by the IS against its enemies. In the framework of the article, the writer explained that in ancient times the Prophet of Islam recognized the importance of deterring the enemy. For instance, the writer said that before the capture of the city of Mosul, the organization distributed clips from its training exercises alongside threats, which caused Iraqi soldiers to flee from the city. In order to strengthen the ISIS's psychological warfare, the writer suggested that its supporters open fictitious Facebook accounts in order to deter Iraqi army soldiers and Popular Mobilization Forces by planting the organization's publications on their accounts. In addition, the writer recommended distributing false information, explaining that it is permissible to lie in a state of war.[10]

Defensive Tactics

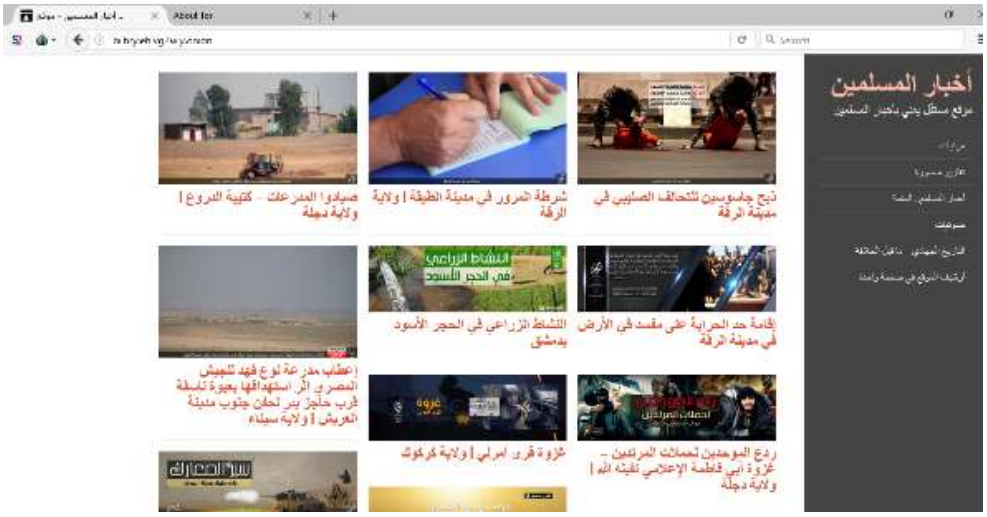
Terrorist organizations, aware of the tireless preventative efforts of security agencies, continued to distribute guidelines and instructions, and continued to move to the darknet where they claimed to be better able to protect the traffic and anonymity of the organizations themselves, as well as their supporters, from the tracking software of

[9] 26.06.16 https://justpaste.it/vgxp
[10] 15.06.16 https://justpaste.it/val5

intelligence agencies and activists who operate against terrorist organization on the Internet in general and on social networks in particular.

Cyber Defense Activities

- A blog by IS supporters that gathers information about the organization's publications moved to the darknet in order to improve the survivability and anonymity of its server and its users.[11] The Website is called "The Muslim News"[12] and is portrayed as an "independent Website that focuses on Muslim news", but in practice it contains the official content and publications of the ISIS, including the flag of the organization displayed on the site's Favicon (Favorites icon). In addition, Twitter accounts affiliated with the organization were discovered that distributed links to various publications that were posted on the Website. It should be noted that the site operates through frequently changing onion addresses.



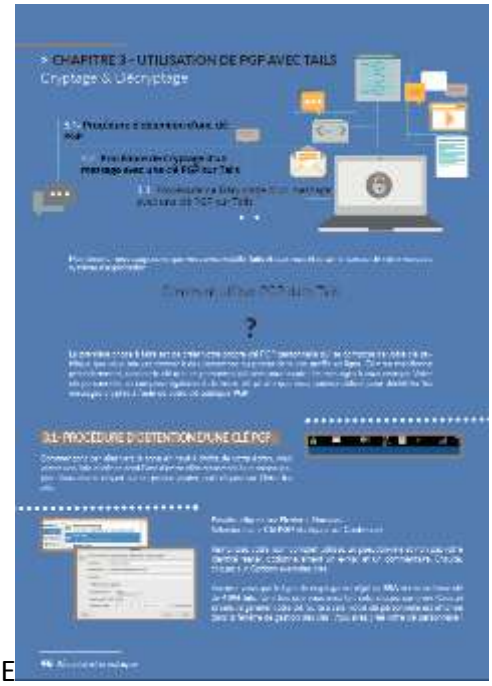
A screenshot of the Website

Cyber-Defense Guidebooks

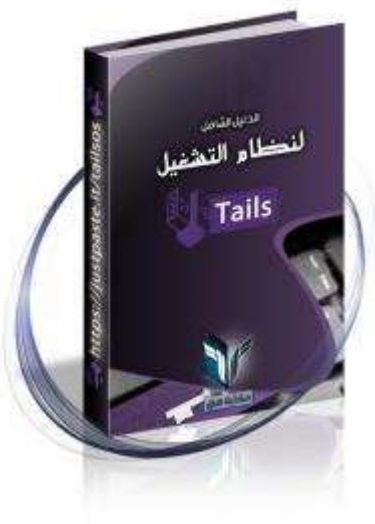
Organizational support for cyber-defense continued with the translation of guidebooks produced by elements unconnected to terrorism, and with the independent production of guidebooks, instructions and warnings about malware:

[11] June, 2016. http://bilbryiehlvg2wiy.onion/
[12] http://dabiq24may2016.ml

- The publication of ISIS's French-language magazine, *Dar al*-Islam, which contained two pages with tips and rules for secure PC use and Internet surfing.[13]



- The publication of guidebooks about cyber-defense on the Telegram channel of the "Electronic Horizon Foundation, which is identified with the ISIS:
    - A guidebook regarding the installation of the Tails operating system, which is considered by the organization to be the best means of preventing electronic monitoring and secure surfing on the Internet.



[13] 26.4.16.

- An announcement regarding a refresher course on the topic of mobile phone security and an application called Locker, which deletes files when an incorrect password is entered when logging on to a cell phone.

- A video titled, "Cyber Warfare 2", which warns the mujahideen about the tracking software used by intelligence agencies on the Internet and on social networks, and calls on them to acquire the technological know-how in order to cope with it.

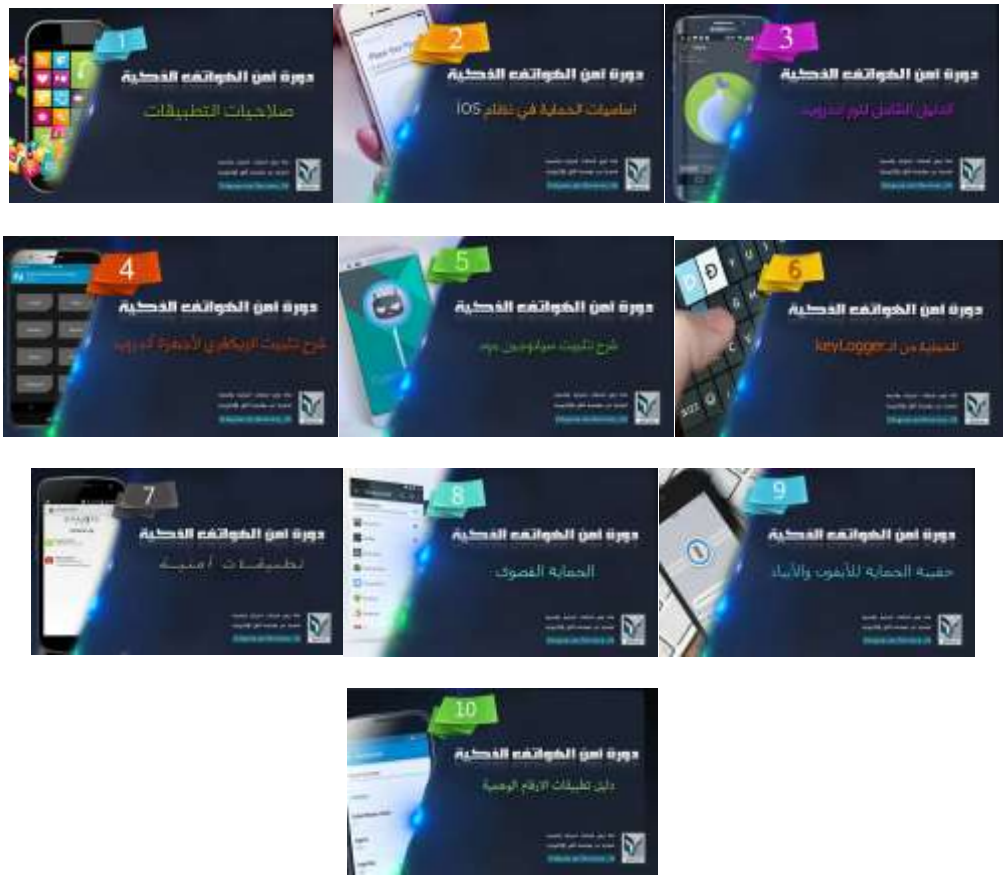
The banner of the "Cyber Warfare 2" video

- A series of lessons in a cell phone security course, including: application authorization (lesson no. 1); secure use of IOS devices (lesson no. 2); Tor use (lesson no. 3); an explanation about recovery (lesson no. 4); an explanation about the use of the CyanogenMod operating system designed for Android devices (lesson no. 5); guarding against the KeyLogger software designed to track users (lesson no. 6); applications to secure mobile devices (lesson no. 7); the use of a

Domain Name System (DNS) as a key protection component of cellular devices (lesson no. 8); an introduction to mobile device security software, such as VPN, ProtoMail and Onion Browser (lesson no. 9); a guidebook on how to use fictitious telephone numbers (lesson no. 10); encrypting files on Android devices (lesson no. 11); a guidebook on how to permanently remove Google services from Android devices (lesson no. 12); a guidebook about an application for sending encrypted text messages called "signal" (lesson no. 13); an explanation on how to change the IP address of Media Access Control address on Android devices (lesson no. 14); an explanation on how to install APK EDITOR to fix Android applications (lesson no. 15); an explanation on how to install the "Threema" encrypted social network (lesson no. 16); a video about digital fingerprints for Android (lesson no. 17). [14]

The banner of the course on telephone security

[14] https://telegram.me/E_HORIZONS



The logo of the "Electronic Horizon Foundation"

- The Telegram channel of the Global Islamic Media Front (GIMF), which belongs to Al-Qaeda, published the following:
  - A list of Websites where there is a risk of being infected with a new virus.
  - Ways to protect against breaches of the WhatsApp encrypted chat application.
  - An update to the surfing public that Instagram accounts are not secure enough and, therefore, there is concern that they can be breached.

- An update on security breaches of the social network, Twitter, for defense purposes.
- A link to an article about software that takes control of a PC and encrypts its files (RANSOM), and how to guard against it.[15]

A screenshot from Telegram

Offensive Tactics

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

- The Head of the US Army Cyber Command, Admiral Michael Rogers, expressed concern during his testimony before the Senate Armed Services Committee in April 2016 that the ISIS would develop information manipulation capabilities, including the disruption of military information traffic by broadcasting false information during battle. Admiral Rogers also raised concerns that a terrorist organization or country could manage to breach the electricity systems in the United States. According to him, organizations like Al-Qaeda and the IS do not yet have significant cyber-attack capabilities but they would have no difficulty recruiting the right people should they choose to focus on that

[15] https://telegram.me/GIMF_Tech1

mission. [16]

During the period under review, the following activities were identified:

- The Telegram channel of "Technical Department of the GIMF", which belongs to Al-Qaeda, published details about a security breach of the Windows operating system when running remote applications, and ways to breach the WhatsApp encrypted chat applications. The publication of security breaches indicates that efforts are being made by terrorist organizations to promote cyber-attacks and their potential methods of execution.
- In June 2016, a member of the Sons of Caliphate - United Cyber Caliphate Army, an umbrella organization composed of several hacker groups identified with the IS, published a video in which he boasted that his organization had successfully hacked into Twitter and Facebook accounts. In addition, he made threats against the founders of Facebook and Twitter, Zuckerberg and Dorsey, should they continue to remove IS-related content and accounts.

The logo of the Sons of Caliphate - United Cyber Caliphate Army

- In early June 2016, a new IS-supporting Telegram was launched under the name "Brigade Alangmasie" (a nickname for suicide fighters who submerse in enemy's line with no intent to come back alive). According to the group, the channel was aimed at bringing down Telegram channels belonging to Shi'ite Muslims on a daily basis. The Telegram

[16] http://www.usatoday.com/story/news/politics/2016/04/05/cyber-commander-fears-data-manipulation-islamic-state-other-enemy/82654786/

account was closed shortly after its launch. [17]

- An IS-supporting Telegram channel called "Ghuraba" was also opened in June 2016 and called for the "downing" of Telegram channels that spread information criticizing the organization. It also published information about those channels.[18]

The "Ghuraba campaign"

- During the period under review, various publications were posted on the justpaste.it Website under the name, "Islamic Cyber Army", which is composed of IS-supporting groups and individuals operating mainly in the field of cyber-attacks. The publications described some of the attacks that were carried out by these agents from which the following information was gleaned:
    - On April 3, a list of email addresses and telephone numbers was published, as well as a list of email addresses and passwords, mostly belonging to Israelis. It should be noted that the list was previously published by a hacker named K1NG ALB in the framework of OpIsrael 2015.
    - On April 8, a list of email addresses and passwords, mostly belonging to Israelis, was published. This list was also previously published in the framework of OpIsrael 2015.
    - On April 8, a list of Facebook accounts that were hacked and breached was published, as well as a list of Facebook email addresses and passwords. The current list was published by hackers named Lion and AnonGhost. It should be noted that the list was previously published by the AnonGhost hacker group in the framework of the OpPetrol campaign.
    - On April 14, a list of Websites that were hacked as part of Website defacement

[17] https://telegram.me/BrigadeAlangmasie
[18] https://telegram.me/hamltgorabaa

activity, mostly in Israel, was published. In addition, the Facebook account details of Israelis, including email addresses and passwords, were published. These lists were published by hackers named Lion, Anony ghost, Engisis & D.r isis. It should be noted that these lists were also published in the framework of OpIsrael 2016.

- On April 14, a list of Facebook email addresses and passwords, most of which apparently belonged to Israelis, was published in the framework of OpIsrael 2016. This list was previously published by AN0N.PH03N1X.
- On April 14, a list of Websites that were allegedly hacked was published. It should be noted that some of details included in this list were previously published by XtReMist and a sample examination revealed that a large part of the Websites are no longer active.
- On April 17, a list of Israeli Websites that were allegedly breached by hackers named cyber & lion & AnonGhost was published. It should be noted that this list was previously published in the framework of the OpPetrol campaign.
- On April 22, a list of Israeli Websites, email addresses and passwords, as well as modem router IP addresses and passwords that were allegedly hacked was published by cyber & lion & AnonGhost. It should be noted that most of this information was previously published in various frameworks.
- On April 22, a list of email addresses, passwords and Websites that were allegedly hacked was published by cyber & lion & AnonGhost. It should be noted that some of these Websites were previously published by AnonCoders.
- On April 22, a price list of performances by international artists was published by cyber & lion & AnonGhost. It should be noted that the list was previously published in several sources, including Pinterest accounts.
- On April 24, a hit list was published [19] that included the personal details of Saudi government/security forces personnel.
- On April 27, the database of an Israeli weapons trading company named FAB Defense was published, including various personal details such as names,

[19] For further information, see: Cyber Desk, “"Killing Lists" – The Evolution of Cyber Terrorism?”, *ICT*, 15.7.16https://www.ict.org.il/Article/1793/killing-lists-the-evolution-of-cyber-terrorism

addresses, contact information, etc. In addition, a list of mostly Israeli Websites that were hacked was published. It should be noted that the list was previously published in the framework of OpIsrael 2015.

- On May 1, a list of email addresses and passwords allegedly including Facebook accounts of Americans was published in the framework of OpUSA. An examination of the list indicated that it included accounts belonging to Israelis. It should be noted that the list was previously published by CDO Cyber Army.
- On May 3, a PHP script used for attack was published. It should be noted that the script had been previously published.
- On May 10, two lists of Websites that were breached and defaced in the framework of OpUSA were published. It should be noted that the lists were published in 2013, one by AnonGhost Team and the other by Chahid injector and Đr'SaMim.
- On May 11, lion and AnonGhost published a list of Israeli Websites that were allegedly hacked, most of which are not active. It should be noted that the list was previously published in the beginning of May by "hacker knights", an Algerian group that supports the IS.
- On May 13, several lists of Websites that were hacked and defaced were published. It seems that these lists were previously published and then combined. Most of the links are no longer active.
- On May 13, a list of email addresses was published. It should be noted that the list was allegedly previously published by AnonSec Team.
- On June 13, screenshots and a list of Twitter accounts that were hacked and defaced by Lion & Ghost were published. At least some of the accounts were indeed hacked and a photo that read, "We are the hackers of the Islamic State" was posted to the accounts.
- On June 13, Lion & Ghost published a list of Websites that were allegedly hacked by "Deep Web". The list, which included the onion addresses of sites on the Tor darknet, had been previously published. Some of the sites are not active.

The following is a collection of selected screenshots of publications from the Justpaste.it Website:

A post from April 3, 2016: A screenshot including leaked personal details

Websites that were attacked

A post from April 26, 2016: A screenshot including a hit list

A post from June 13, 2016: A screenshot including documentation of accounts on social networks that were hacked

Review of Organizational Activities

ISIS

During the period under review, ISIS fighters and supporters continued to use the Internet platform for various activities, including to leak information as part of its "psychological warfare" and as a base for offensive operations and attacks on Websites and social network accounts.

Among the range of uses discovered during this period, it is worth noting the launch of designated Telegram channels, the continued dissemination of messages, references to sites on the darknet, and a focus on children through an application for learning the Arab alphabet accompanied by militant photos.

During the period under review, ISIS fighters published a list of attacks allegedly carried out by its members as well as the information gleaned from them. Some of this information included previously published lists, some of which came from open information sources and/or were previously leaked and re-published by ISIS supporters. In addition, it seems that the breach, if indeed there was one, focused on small Websites, most of which returned to normal operation. The breaches of social network accounts included the defacement of profile pages, the publication of messages of support for the ISIS and the leak of account owners' details, including email addresses and passwords. A hit list was also published [20] that included details about military personnel in Saudi Arabia. An analysis of the attack targets indicated that ISIS supporters are concentrating efforts against Internet sites in Israel, the US and India.

It should be noted that one member of the organization's cyber groups published threats against the founders of Facebook and Twitter should they continue to remove ISIS-related content and accounts.

Al-Qaeda

The organization's technological department placed special emphasis on cyber defense

[20] For additional reading about the publication of "hit lists", see: https://www.ict.org.il/Article/1793/killing-lists-the-evolution-of-cyber-terrorism

measures, including the publication of guidelines and updates regarding security breaches. In addition, the department published details about security breaches through which attacks can be launched.

Cyber-Crime and Cyber-Terrorism, April-June 2016

Recent years have seen an increasing number of cyber-attacks against political targets, critical infrastructure, and the Websites of commercial corporations. These attacks, which receive increasing amounts of international attention, are perpetrated by states (which do not claim responsibility for them), groups of hackers (such as Anonymous), organized crime and lone hackers. We believe that terrorist organizations are working in close collaboration with organized crime to learn from their attempts [at cyber-crime] and may even be hiring their services. In light of this, it is important to examine and analyze cyber-crimes attributed to criminal organizations, as well as new development trends and patterns. The following information was culled from the visible (OSINT) and invisible ("Dark Web")[21] Internet between April - June 2016.

Trends in Counter Measures

- US Deputy Secretary of Defense, Robert Work, announced that the US Cyber Command is operating against the ISIS in an innovative manner by using "cyberbombs" to disrupt command and control operations as well as communications systems in an effort to disrupt the organization's recruitment, propaganda and fundraising activities. [22] Later, US Director of National Intelligence, James Clapper, claimed that while the campaign is creating confusion among members of the organization, there is still a long way to go. [23]
- A 20-year-old Kosovan citizen named Ardit Ferizi, known as Th3Dir3ctorY, was sentenced in the US to 20 years in prison for providing assistance to the ISIS. Ferizi was convicted of

[21] The "dark Web" or darknet is "A collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks." See P. Biddle, P. England, M. Peinado and B. Willman (no date), "The Darknet and the Future of Content Distribution", *Microsoft Corporation*, http://msl1.mit.edu/ESD10/docs/darknet5.pdf.
[22] http://www.foxnews.com/politics/2016/04/25/cyber-command-opening-up-new-front-against-isis.html
[23] http://www.voanews.com/a/cyber-war-versus-islamic-state-work-in-progress/3336773.html

hacking into computer systems[24] on July 13, 2015 and transferring the details of 1,351 US government and army personnel to Junaid Hussain (aka Abu Hussain al-Britani), a member of the IS, who published the information on August 11, 2015. [25] It should be noted that Ferizi was arrested by Malaysian authorities at the request of the US in October 2015.

The Legal Battle against Terrorist Activity on the Internet

The legal battle against terrorist activity on the Internet in general, and on social network platforms in particular, is the most problematic. One problem has to do with the legal authority of a state and its courts system to direct the owners of various platforms to perform or refrain from action. Such a directive may not hold any relevance due to the absence of territorial jurisdiction and, even worse, may contradict the provisions of national law in another country where the owners of the platform operate.

One method of dealing with this issue that is gaining momentum is the filing of tort claims against platform owners by those who feel they have been victims of terrorism promoted one way or another by the platform in question. These are civil claims that often "override" the limitation of state territorial jurisdiction in order to take criminal action against platform owners.

Another method of dealing with this issue was demonstrated by Microsoft, which published its approach to terrorist content online in May 2016,[26] according to which it prohibits the publication of hate speech and support for violence in its products and is working to remove them. The company announced that, in the absence of an agreed-upon definition of terrorism, it recognizes the United Nation's sanctions list of terrorist organizations as an official document in terms of content and will continue its notice-and-takedown activities to remove content per the request of visitors or government officials, through the use of an online form. [27] Microsoft added that it will cooperate with government officials to block

[24] https://www.justice.gov/usao-edva/pr/isil-linked-hacker-sentenced-20-years-prison
[25] http://www.militarytimes.com/story/military/crime/2016/06/15/guilty-plea-terrorists-hack-us-military-information/85925644/
[26] http://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.0000kfya4rdple63rvn29364br1vm
[27] http://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/

terrorism-related content related to the country in which they operate by removing them from the Microsoft search engine, Bing, as it claimed to already be doing with police forces in France. The company also claimed that it was examining the possibility of expanding its cooperation with NGOs on the issue and was funding research by Professor Hany Farid of Dartmouth College to develop technological capabilities for the detection of terrorism-related content.

Legal and Regulatory Developments

Legal and regulatory developments regarding **the use of personal data by governments in counter-terrorism efforts moved ahead between April and June 2016 in several regions of the globe**. The United States, China, the European Union and Russia each published either draft laws or regulations or final legislative acts that will influence these countries' treatment of personal data – one of the controversial tools in the global fight against terrorism.

The general trend is one of increased governmental authority to survey personal data as metadata, or to specifically request the personal data of persons of interest in the context of crime prevention in general, and counter-terrorism in particular.

Countries impose relatively narrower or broader limitations on this governmental authority, depending upon the extent to which personal privacy rights are protected under a given legal regime.

Below is **a brief survey of the developments in the four jurisdictions referred to above**:

I. China

Two developments regarding China's regulation of cyberspace:

- **Draft Cybersecurity Law – Second Reading:** On June 27, 2016, the Standing Committee of the National People's Congress of the People's Republic of China held a **second reading of China's draft Cybersecurity Law**. The draft law provides *inter alia* for increased governmental supervision of digital network operators, which will be required "…to comply with social morals and business ethics, and will be subject to governmental and public supervision. In addition**, network operators will be required to preserve web logs for at least six months, and cooperate with the supervision and inspection of competent government authorities.**" Under the

second draft, **network operators will be required to comply with social morals and business ethics, and will be subject to governmental and public supervision.** In addition, network operators will be required to preserve web logs for at least six months, and cooperate with the supervision and inspection of competent government authorities.

- **Administrative Provisions on Internet Information Search Services:** On June 25, 2016, the Cyberspace Administration published its new Administrative Provisions on Internet Information Search Services, which will come into effect on August 1, 2016. Under the Provisions, **Internet information search service providers (including operators of search engines) are required to adopt information security management systems**, "…such as systems enabling the review of information, real-time inspection of public information and protection of personal information". They are prohibited from showing subversive and obscene content and other content prohibited by law and regulation. Should legally-prohibited content shows up in a search result, the result should be blocked and reported to the Cyberspace Administration.

II. Europe

The publication of the EU General Data Protection Regulation ("GDPR") and adoption of the Network Security Directive took place in May and the beginning of July, respectively.

- Publication in the Official Journal on May 4, 2016 of the **EU General Data Protection Regulation ("GDPR")** following the Parliament's voted for adopting the GDPR on April 14, 2016. The signing of the final draft on April 27, 2016. The GDPR entered into force 20 days following its publication and its provisions will be directly applicable in all EU Member States two years after this date, on May 25, 2018. [ramifications TBA]
- The **Network Security Directive,** adopted on July 6, will impose security obligations on "operators of essential services" in critical sectors and "digital service providers." These operators will be required to take measures to manage cyber risks and report major security incidents. [ramifications TBA]

III. USA

- Aftermath of FBI v. Apple

- **Privacy and Civil Liberties Final Guidelines**: **Cybersecurity Information Sharing Act of 2015 ("CISA")**[28]. This document was published on June 15 by the Department of Homeland Security and DOJ pursuant to Section 105(b) of CISA. It establishes privacy and civil liberties guidelines governing the receipt, retention, use and dissemination of cyber threat indicators and defensive measures by federal entities under CISA. "**Federal entities should follow requirements to safeguard cyber threat indicators, including those containing personal information of specific individuals or information that identifies specific individuals that is directly related to a cybersecurity threat or a use authorized under CISA**, **from unauthorized access or acquisition**. In addition, appropriate sanctions will be implemented for activities by officers, employees, or agents of the Federal Government in contravention of these guidelines."

  Guiding Principles include "Cyber threat indicators provided to the Federal Government under CISA may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of federal law…**solely for authorized activities** as outlined in CISA."

  "Use" guidelines determine that "…federal entities that receive cyber threat indicators and defensive measures under CISA **will use them only for the purposes authorized** under CISA.

  Specifically, cyber threat indicators and defensive measures provided to the Federal Government under CISA may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of federal law…solely for:

  1. **a cybersecurity purpose**;

  2. the purpose of **identifying (i) a cybersecurity threat, including the source of such cybersecurity threat or (ii) a security vulnerability**;

  3. the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, serious bodily harm, or serious economic harm, **including a terrorist act** or a use of a weapon of mass destruction;

[28] https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_(Sec%20105(b)).pdf

Significant Incidents

Attack against the Nuclear Power Station in Germany

In April 2016, W32.Ramnit and Conflicker malware were detected at the nuclear power station in the city of Gundremmingen in Bavaria, Germany (the largest state in Germany with three electricity producing units). The malware was detected on the computer responsible for fuel feed control[29] and on detachable drives, mainly USB sticks and office computers connected to a network separate from the operational one.[30] It can be assumed that these well-known malware[31] were used in order to reach SCADA systems by infecting additional computer stations. The identities of those behind the attack and its objective have not yet been published.

The World-Check Database Leak

At the end of June 2016, Chris Vikery, a cyberspace researcher, published details regarding the leak of the World-Check database belonging to Thomson Reuters. This database includes over two million lists of terrorism suspects drawn from open sources among various countries. [32] The database is designed to serve government agencies, the financial sector and other parties that need to verify identities and work to prevent money laundering and terrorism financing.[33] Vikery believes that the information was exposed due to the incorrect installation of the database that enabled public access to the data. Later, it was published that the database could be purchased in a store for illegal trade on the dark net for several thousand dollars.[34]

Case Study – Fraud using SWIFT Money Transfers - Chronicling Many Years of Complacent Disillusionment

The first crack in the fortified wall of money transfer services through SWIFT was brought to

[29] http://www.br.de/nachrichten/schwaben/inhalt/kkw-gundremmingen-schadsoftware-akw-100.html
[30] http://www.telegraph.co.uk/news/2016/04/27/cyber-attackers-hack-german-nuclear-plant/
[31] https://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99
[32] https://risk.thomsonreuters.com/en/products/world-check-know-your-customer-b.html
[33] https://www.reddit.com/r/privacy/comments/4q840n/terrorism_blacklist_i_have_a_copy_should_it_be/
[34] http://motherboard.vice.com/read/hacker-leaked-terrorism-watchlist-world-check-sold-dark-web

public attention in general, and to the attention of the cyber-defense and information security communities in particular, on April 25, 2016.

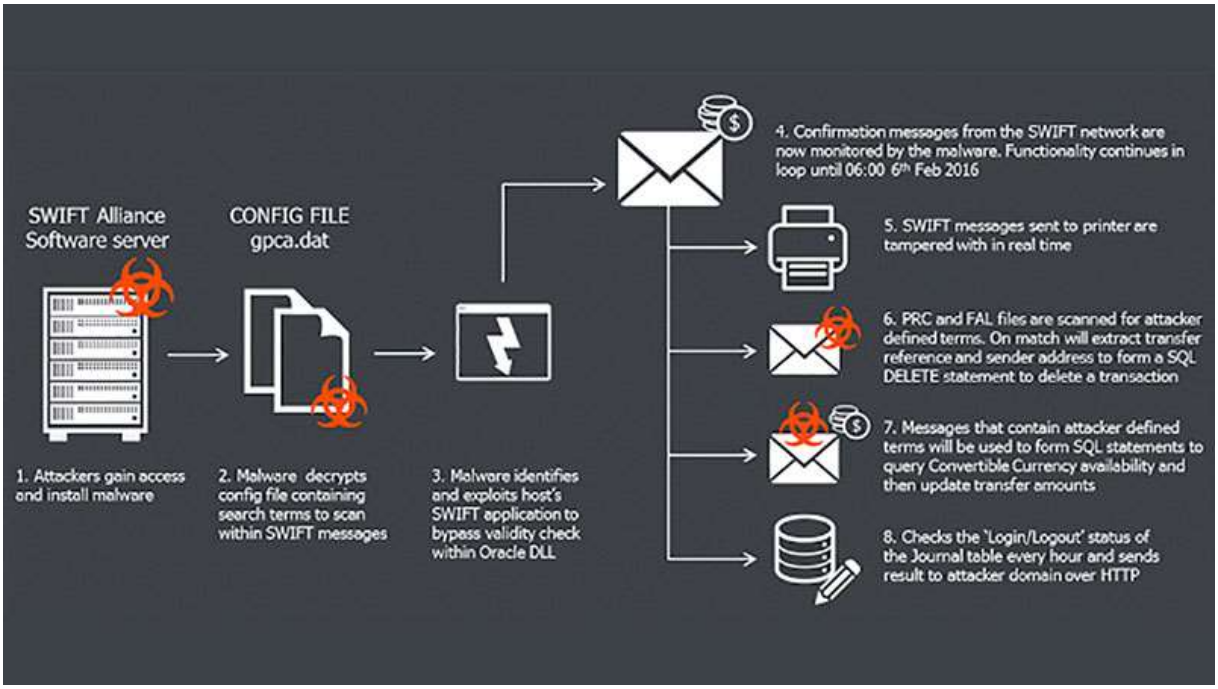
The company, SWIFT, has operated since 1973 as a junction for money transfers through messages between 11,000 financial institutions operating from approximately 200 countries around the world. The money transfers are carried out for the customers of financial institutions, including private individuals, businesses and governments, making it an organization with a very high financial turnover.

In February 2016, it was published that approximately 81 million dollars was withdrawn from the Central Bank of Bangladesh using four fake transfers on SWIFT systems, "only a small" part of the approximately one billion dollars that the attackers intended to transfer for their use.

This news item grabbed headlines on news Websites, economy columns, news about the banking sector and, of course, technology and information security Websites. One site, www.bankinfosecurity.com, which focuses on information security issues in the field of banking, published the details that were known and through which one could follow the developments in the case during the six months since it was reported:

BAE Systems Applied Intelligence[35], the security company that investigated the incident, found that a sophisticated malicious code had been inserted into the banking system in Bangladesh that enabled the fake transfers and simultaneously "took care of" deleting alerts and records that leave traces so that bank employees had no indication of the transfers that were made. The money was transferred to a bank in the Philippines and from there the money was withdrawn in cash from casinos operating in the country.

[35] http://www.databreachtoday.com/converging-against-fraud-industry-a-8584



A scheme about the attack published by BAE Systems[36]

The initial fear was that the central systems of the SWIFT company had been attacked, but it was later clarified that a malicious code had been injected into the banking systems in Bangladesh that had interfaces with SWIFT systems or that took part in presenting reports on transactions made via SWIFT. The complexity of the attack indicated that the attackers were very well acquainted with the bank systems and with the SWIFT work protocol.

The initial response by SWIFT, the day after the report, maintained that it was an information security problem at the bank that was attacked and not a breach of the SWIFT systems. Nevertheless, the company announced that it would help the banks that use its services by issuing guidelines to increase the security level, including and in the context of SWIFT systems.

The next day, SWIFT announced that it was aware of additional incidents of attacks against other banks that created fake money transfers and it issued a security patch to all of its customers designed to warn of attempts to cover the tracks of transfer actions made on the system. At the same time, the company issued updated security guidelines to all of its customers.

[36] http://baesystemsai.blogspot.co.il/2016/04/two-bytes-to-951m.html

Approximately two weeks after the initial report, SWIFT revised its communication to its customers, retracted its position according to which there had been no breach of the SWIFT software but rather a sophisticated fake code whose penetration of banking systems enabled the unauthorized use of SWIFT systems, and therefore demanded that the banks belonging to the network increase their monitoring and security measures.

In addition, the Symantec cyber-security company[37] published an assessment according to which there is was link between the attackers and the method of attack, and the agent responsible for carrying out the attack against SONY Pictures' systems in December 2014.

Less than a month after the initial report, and due to the fact that it was not an isolated incident but rather a chain of events in which a malicious code was inserted in banking systems to make fraudulent transfers, government and regulatory authorities of the banking system in various countries demanded that banks using SWIFT systems perform additional checks and controls, and ensure the implementation of SWIFT's security guidelines.

The issue was also raised by the House Committee on Science, Space and Technology, which referred a question to the Federal Bank regarding the bank's preparedness as a result of the incidents that were published and additional incidents should they take occur.[38]

On May 24, 2016, about one month after the initial report and following repeated attempts by SWIFT to place responsibility for the fraud on the low level of security of the bank systems that were attacked, the CEO of SWIFT made a statement according to which the company intended to improve its systems' level of security, to provide banks with additional tools to help them detect scams that use SWIFT, and to share information regarding such attempts in the future should they occur.

On July 4, 2016, following reports of six incidents in which fraudulent money transfers were made using SWIFT systems (the last of which was an attack on a bank in the Ukraine during April), the company issued an announcement to its clients according to which its systems were already exposed to the malicious code performing fraudulent transfers and, therefore, they must act to detect signs of its existence. This announcement increased activities undertaken by financial and regulatory agencies in the financial sector for a thorough

[37] https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks
[38] http://nypost.com/2016/06/01/congress-launches-investigation-into-81m-cyber-fraud/

inspection of the systems and the risks derived from their method of operation in various institutions.

On August 17, 2016 Reuters news agency published a special report [39] regarding the fraud carried out using SWIFT systems and turned the spotlight on the company's management that carelessly addressed the low level of security at small banks and institutions. Only the accumulation of incidents that were revealed in 2016 caused the company to recognize the need to strengthen the security level of the system in general, and the security level in terms of customer access to system services particular. On September 20, 2016 SWIFT announced that, starting at the end of this year, it would provide its clients with an optional daily service to examine irregular transaction patterns suspected of fraud on a different track than the regular messaging system. In this format, customers will be able to receive alerts of suspicious activity even if SWIFT's standard alert mechanisms are silenced.

On September 27, 2016 - four months after the initial report of fraud using SWIFT systems, SWIFT announced that it would activate a mandatory security standard for all of its customers. Enforcement of the standard will begin in the second quarter of 2017, in the framework of which organizations will be obligated to perform an annual self-assessment of compliance with security standards, and to report their findings to SWIFT as well as to the regulators in the relevant sectors.

The snowball of fraud incidents using SWIFT systems began to roll in April 2016 and since then it has gained momentum, added more and more banks that fell victim to these schemes, and completely changed customers' perception of the security level of the SWIFT systems themselves and the components of the security level that they are supposed to provide to their customers, which affects confidence in the entire mechanism.

The attacks, which were carefully planned, were apparently based on first-hand knowledge of SWIFT systems and the systems of the various banks that were attacked, and were scheduled for a series of days of inactivity at the banks involved. The attacks included elements of inserting arbitrary code, executing transfer activities and disrupting the control mechanisms in a manner that covered up traces of the actions that were performed.

[39] http://www.reuters.com/article/us-cyber-heist-warnings-specialreport-idUSKCN10S0WC

The attacks also had a non-technological component that included the opening of bank accounts to which the money transfers were made and from which the money was transferred immediately and in cash to parties such as casinos that were accomplices to the fraud. The properties of such large-scale fraud and attacks point to organized crime as the perpetrators. However, terrorist organizations can also use this method to raise funds to finance their activities.

ICT Cyber-Desk Team

Dr. Eitan Azani, Deputy Executive Director, ICT

Dr. Michael Barak, Team Research Manager, ICT

Adv. Uri Ben Yaakov, Senior Researcher, ICT

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

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

Nir Tordjman, Cyber Desk Team Research Manager, ICT

ABOUT THE ICT

Founded in 1996, the International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world, facilitating international cooperation in the global struggle against terrorism. ICT is an independent think tank providing expertise in terrorism, counter-terrorism, homeland security, threat vulnerability and risk assessment, intelligence analysis and national security and defense policy. ICT is a non-profit organization located at the Interdisciplinary Center (IDC), Herzliya, Israel which relies exclusively on private donations and revenue from events, projects and programs.

ABOUT ICT CYBER-DESK

The Cyber Desk Review is a periodic report and analysis that addresses two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse) and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack). The Cyber Desk Review addresses the growing significance that cyberspace plays as a battlefield in current and future conflicts, as shown in the recent increase in cyber-attacks on political targets, crucial infrastructure, and the Websites of commercial corporations.

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

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