IDC HERZLIYA

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

ICT Cyber-Desk

PERIODIC REVIEW

Cyber-Terrorism Activities

Report No. 16

January – March 2016

Highlights

This report covers the period of January - March 2016 and covers 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 following are among the issues covered in this report:

- The continuing trend of publishing information security guidelines and recommendations, including information and recommendations for correct methods of operation and software manuals, or services with a high encryption or anonymity level.
- Terrorist organizations continue to publish information about the dangers of intelligence and law enforcement officials who operate on the Internet to search for and locate terrorism supporters. In addition, all supporters are called on to continue spreading the organizations' messages and guidelines for proper work.
- Officials in jihadist organizations continue to spread Best Practice guidebooks on the Internet and guidelines for using software and applications to increase information security. These are mainly used to encrypt data on the device and/or for data trafficking and maintaining the anonymity of Internet users. In addition, manuals for video processing are found. As previously stated, in recent years organizations have been using a wide range of software in order to create visual content at a professional level.
- Terrorists and terrorism supporters continue to hack Internet sites, especially as part of defacement attacks. In January 2016, Islamic State activists tried to recruit hackers to hack into government databases for pay. In February 2016, a television interview in Lebanon reported the existence of a Shi'ite hacker group, affiliated with Hezbollah, named Kadimon (translation – we are coming). The article raised the claim that members of the group had successfully hacked into security cameras throughout Israel, including cameras at the Ministry of Defense at the government offices campus in Tel Aviv.

- Following the terrorist attacks in Europe, it seems that the European Union is re-evaluating the growing threat posed by the Islamic State. In addition, the launch of a US cyber campaign against the organization is reported in February, aimed at disrupting and even restricting the Islamic State's ability to operate on the Internet. It should be noted that cooperation between countries and companies, such as Twitter, has been successful in removing IS content from the Internet.
- Ransomware continues to pose a major threat from cybercrime organizations, and the trend of malware expansion continues to affect additional systems and devices, including Android mobile devices. In addition, there was an increase in the sale of ransomware-as-service, in which advanced malware can be purchased or downloaded to launch an independent attack.

Table of Contents

Highlights 2

Electronic Jihad 5

- Key Topics of Jihadist Discourse, January-March 2016 5

  Al-Qaeda 5

  Al-Qaeda in the Arabian Peninsula 5

  Al-Qaeda in the Islamic Maghreb 6

  Al-Nusra Front 6

  Al-Qaeda in the Indian Subcontinent 6

  The Islamic State 7

  Miscellaneous 8

- Jihadist Propaganda 8
- Defensive Tactics 11
- Offensive Tactics 18

Review of Organizational Activities 20

- Islamic States Affiliates and Supporters 20
- Al-Qaeda in the Indian Subcontinent 22
- Hezbollah 22
- Hamas 23

Cyber-Crime and Cyber-Terrorism, January-March 2016 24

- Major Cyber Incidents 25
- Counter Measures 29
- Ransomware 33

Case Study – "Killing Lists" – The Evolution of Cyber Terrorism? 34

Electronic Jihad

Global jihad groups are increasingly venturing into cyberspace. Their use of the Internet for "typical" activities – communication, recruitment of operatives, fundraising, propagandizing, incitement to hatred and violence, intelligence gathering, and psychological warfare – is well-established. In recent years, global jihad and other terrorist organizations have begun to use cyberspace as a battleground for what they call "electronic jihad", attacking the enemy by sabotaging its online infrastructure, using the information available to them from the virtual world to cause mayhem in the real world, and developing their own defensive capabilities against cyber-attack. Following is a selection of recent key acts of electronic jihad, and a brief overview of the key themes reflected in jihadist discourse and propaganda.

Key Topics of Jihadist Discourse, January-March 2016

Al-Qaeda

The execution of several Al-Qaeda operatives who were being held in Saudi prisons, at the start of January 2016, sparked widespread discourse against the Saudi regime among the most senior ranks of the organization and among jihadists on social networks. The discourse was mostly characterized by calls for revenge and a description of the Saudi regime as an infidel regime that denies the religion of Islam, and betrays its duties towards Muslims through, among other things, its association with the US, which is waging an all-out war to weaken Islam's strength. Sheikh Ayman al-Zawahiri, the leader of Al-Qaeda, called on Muslims, especially clerics, in the Arabian Peninsula to revolt against the Saudi regime and to avenge this and other crimes committed by the Saudi regime. Al-Qaeda branches in North Africa and Yemen also made similar calls and threats to respond with revenge attacks, and jihadists on social networks described in detail the "crimes" committed by the regime towards the Muslim Nation while calling for revenge.

Al-Qaeda in the Arabian Peninsula

Al-Qaeda in the Arabian Peninsula (AQAP) emphasized that the main enemy of

Muslims and Islam is the US and, therefore, the focus must be on weakening it. In this context, Sheikh Khaled Batarfi, a senior AQAP leader, called on the mujahideen and on Muslims living in the US to focus efforts on attacking targets on US soil. In addition, the organization emphasized the importance of maintaining unity among the ranks of the mujahideen in Syria and their devotion to the mission until victory is achieved, and he warned them about their enemies' attempts to cause a rift among them.

Al-Qaeda in the Islamic Maghreb

The beginning of 2016 was characterized by a significant intensification of AQIM's propaganda machine. Emphasis was placed on the issue of freeing western captives being held by the organization in exchange for the release of Muslim prisoners being held in western jails – a recording was published that clarified the conditions of release for two captives, a Swede and a South African who were captured by the organization in 2011 in Timbuktu, in Mali. Special emphasis was also placed on threatening to attack interests in France and its allies until it is driven out from Muslim lands, especially in Mali. In this context, the organization claimed responsibility for a terrorist attack that was carried out against several tourist attractions in Burkina Faso as well as a tourist site in eastern Abidjan on the Ivory Coast, in revenge for "Crusader" attacks on Muslims and as a message to local regimes not to cooperate with France.

Al-Nusra Front

The launch of peace talks in Geneva between the Syrian regime and rebel factions aimed at implementing a ceasefire sparked sharp criticism from Al-Nusra Front, Al-Qaeda's branch in Syria. Sheikh Abu Mohammed al-Julani criticized the talks and called on Al-Nusra Front fighters, as well as those from other rebel factions, to increase their attacks against Syrian security forces.

Al-Qaeda in the Indian Subcontinent

Al-Qaeda in the Indian Subcontinent intensified its PR activities by launching a new series of publications titled, "Al-Hadid". In the framework of the series, propaganda

materials were published regarding the activities of members of the organization and accusing the Pakistani regime of massacring and persecuting civilians.

The Islamic State

Against the backdrop of the Islamic State's loss of power and territory to its enemies, the organization launched a PR campaign aimed at raising its fighters' morale and emphasizing its military achievements in the other provinces under its control. For example, it praised the fighting spirit of its soldiers following the loss of Ramadi, and praised their success in expanding Libya's foxhole. Against the backdrop of the organization's failed attack to seize control of the Tunisian city of Ben Gardane, the organization praised the attack and encouraged the execution of more jihad attacks on Tunisian soil.

Alongside this trend, the organization continued its efforts to recruit new fighters to its ranks. On January 19, 2016 it launched a network campaign that called on Muslims in North African countries, specifically Tunisia, Morocco, Mali, Algeria, Libya and Mauritania, and even called on members of Al-Qaeda, to join its ranks and assassinate government officials, soldiers and security forces. The organization even called on the Sunni population in Lebanon to join its ranks, called on Christians in Lebanon to convert to Islam, and called on soldiers in the Lebanese army to defect. Special emphasis was also placed on the Caucasus and Russia. According to the organization, if Muslims in these areas are prevented from joining the ranks of the organization, then they should obtain a weapon and attack "infidels" throughout Russia, even using a knife.

In addition, the organization continued to wage a psychological war against the West, especially with threats to carry our revenge attacks on western soil. In *DABIQ* magazine, which is published in English, and in videos that were distributed on the topic, the organization praised the terrorists who carried out the attacks in Paris in November 2015 and vowed to repeat this type of attack in France and other western countries.

The Islamic State branch in the Sinai Peninsula also waged psychological warfare, specifically against the Egyptian regime. A senior IS leader called on Muslims in Egypt to show initiative and rebel against al-Sisi's regime until it is overthrown, to destroy

the Christians, intimidate the Jews and implement shari'a. According to him, jihadists consider themselves committed at the present time to work for the liberation of Palestine, Constantinople and Rome, and not to wait for future generations to fulfill this mission.

Miscellaneous

A group of Egyptian Islamists, some of whom support Al-Qaeda, such as Sheikh Hani al-Sibai, launched a campaign aimed at liberating Egypt from the secular orientation that, according to them, al-Sisi's regime is trying to force on Egypt and to replace it with an Islamic identity as in previous generations.

Jihadist Propaganda

The months of January-March 2016 saw the continued trend of publishing information security guidelines and recommendations, including information and recommendations for correct methods of operation and software manuals, or services with a high encryption or anonymity level. Terrorist entities continued to publish information about the dangers of intelligence and law enforcement officials who operate on the Internet to search for and locate terrorism supporters. In addition, all supporters were called on to continue spreading the organizations' messages and guidelines for proper work.

- "Afaaq [*Horizons*] Electronic Foundation", a cyber group that aligns itself with the Islamic State, published a video titled, "Electronic Warfare and the Carelessness of the Mujahideen". The video addressed the dangers facing jihadists as they surf the Internet, including gathering browsers' information, tracing their habits, locating their physical location, and more.[1]

[1] January 31, 2016. http://salylasayf.allahmuntada.com/t604-topic

The video banner

- On March 16, a new Telegram channel named "Afaaq [*Horizons*] Electronic Foundation" was launched, which focused on publishing guidebooks on how to remain secure in the cyber world. For example, it published a guidebook on how to open Twitter accounts; a guidebook on how to use the Internet anonymously using the Tails OS operating system; a guidebook on how to use Telegram; and more.

- Al-Sabeel jihadist media institution, which belongs to the Shura Council of the Mujahideen in Derna, announced the opening of an account on the Telegram encrypted chat application.[2]

[2] March 17, 2016. https://twitter.com/Assabeel_Media/status/710513302858760192

- A secret channel to attack the tyrants, a special channel designed for Caliphate supporters to combine electronic invasions in order to spread the path and publications of the Islamic Caliphate.[3]
- The "Electronic Army of the Mujahideen" called on visitors to the social network, Twitter, to help spread its publications condemning the involvement of western countries in Libya, focusing on the war crimes being committed against the local population, under the hashtag "#TheCrusaderInvasionAgainstLibya".[4]

Banner calling for help in posting correspondence on Twitter

- The jihadist media group, Muassat al-Nukhba lil-'Ilam, which is involved in publicity for Al-Qaeda, announced the opening of a new account on the social network, Twitter, after its previous account was closed by Twitter management. The account includes articles, opinion statements and propaganda materials by Al-Qaeda.[5]

[3] October 6, 2015. https://twitter.com/Safyia__22/status/651559848337887232
[4] February 24, 2016. https://twitter.com/farees_alzhrani/status/702546631904894977
[5] March 10, 2016. https://twitter.com/massagesnokbah/status/708081492954628096

The banner of the media group's Twitter account

Defensive Tactics

During January-March 2016, jihadist organizations and groups supporting them published official guidebooks for various software and applications to increase information security. These applications are mainly used to encrypt information on a device and/or to traffic information, maintaining anonymity of user activity on the Internet. In addition, guidebooks were found for video image processing since in previous years organizations have used a wide range of software in order to create professional-level visual content.

- During January-March 2016, the Telegram channel "Android Applications" published a series of applications enabling the encryption of voice calls, text message exchanges and other means of communication, as well as secure browsing in cyberspace using Android devices. The recommended applications included:
    - RedPhone application – encryption software for voice calls.
    - vyprvpn application – encrypted browsing on the Internet.
    - duckduck – secure search engine.
    - Textnow application – enables the user to obtain a ficticious telephone number from the United States. By using this service, the user is able to bypass the authentication mechanisms using a text message and/or voice call, a mechanism designed to authenticate the identity of the user and even to prevent or limit one's registration to various Internet sites or services.
- The "technical department" of the GIMF media institution, which serves Al-

Qaeda, published several guidebooks on its Telegram channel regarding secure browsing on the Internet, image design software, software for publications distribution on the Internet, and a warning regarding "holes" in the security of various browsers and software.

- The "Technical Committee of Al-Fajr", a cyber-group devoted to developing security and communication tools for jihad fighters, announced the launch of a self-designed Web site that will enable messages to be sent and posted in a more secure manner on Twitter and other interfaces on the Internet, under the address: http://www.fajrtaqnipastemaker.net.[6]

The banner announcing the launch of the above Web site

The Web site enables textual content to be stored anonymously when it is possible to specify the name of the author and title. The site enables the storage of text for a limited time, between five minutes and one hour, allowing the creation of a shortened link for distribution. The site includes an interface in Arabic and in English. The Web site allows the user to comfortably and anonymously disseminate unlimited text. The content is securely stored on the site and can be distributed freely through a long/short link. The site prevents search engines from scanning and indexing the existing pages and, in fact, it is not possible to do a search and view the saved messages.

[6] March 1, 2016. https://www.alfidaa.info/vb/showthread.php?t=115641

A screenshot of the Web site

An example of messages published on the Web site

An example of the distribution of a link on social networks

- The "A'MAQ", Mozila Browser plugin, is a technological solution that was developed by Islamic State supporters in order to preserve the ability to connect to the Web site of the organization's official news agency at any given time despite changes to the URL address. This step illustrates the adaptive approach of IS supporters in the framework of which they adopt existing technologies and

develop new ones in order to overcome the obstacles placed before them by various elements.

Islamic State Web sites serve as a target for attacks by hackers working to disrupt the organization's activities in cyberspace. These attacks include locating the organization's accounts, institutions, operatives and supporters on social networks, and disrupting their activities by attacking them independently or reporting them to the relevant authorities to have them removed. For example, a hacker from the BinarySec[7] group who answers to the name "Rebirth" posted over 100 Web sites allegedly belonging to IS operatives on his Twitter account. According to him, he and others disrupted activity on these sites, some permanently and some only temporarily. Among the sites that were affected were the Islamic State's "Amaq" news agency, whose address was removed from the network again in May 2016.

Illustration no. 1: A Twitter post regarding the downing of the "Amaq" Web site

The series of terrorist attacks ascribed to the Islamic State that were carried out in Europe starting in 2015 led to a significant increase in the number of attacks by hacker groups against the organization, causing the organization's Web sites to alternate rapidly, and in certain cases to be taken offline on the same day that they were put up. This situation makes it difficult for the organization's supporters to maintain the connection and to be updated about its activities due to the change in the URL address.

[7] https://twitter.com/RealRebirth

In order to overcome this problem, IS supporters created the group 'Afaq' (Horizons), an Add-on dedicated to the "A3maq" Web site (the organization's news agency) for the Mozilla browser, which enables direct access to the site without needing the updated Web address. The Add-on index updates the browser automatically with the new address so that the user can access the updated Web address at the press of a button. A detailed guidebook explaining how to install the Add-on was circulated on social networks, including on Telegram channels used by IS supporters. It should be noted that the Add-on was developed for the Mozilla browser, seemingly because it is the default used for Web browsing, using TOR software that IS supporters are instructed to use in order to maintain anonymity and protect themselves from law enforcement authorities and intelligence agencies.

This step by IS supporters demonstrates its efforts and capabilities for coping with and overcoming the obstacles placed before them. The creation of the Add-on indicates that the organization will continue to act adaptively and creatively in order to maintain contact with all of its supporters and operatives on the Internet.

The following is a translation of the Add-on installation guide:

Browser Add-ons work to adjust the browser settings in line with the aspirations of the users. There are many useful security add-ons for browsers that we've already discussed here.

However, the arbitrary policies of the browser stores on Chrome and Firefox prevent the distribution of some add-ons. To overcome this problem, you can install the add-ons manually.

To install A3maq Agency add-on to Firefox press here.

Press on Add-ons:

- *Press on the gear icon ⚙ and then press on "Install Add-on from File"*

- *Press on "Install" to install the add-on on the browser*

- *Press on the icon shown in the next picture to browse A3maq Web site*

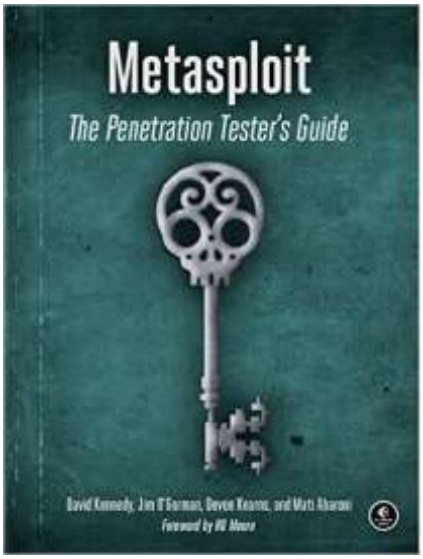
- *The website will open as shown in the next picture:*

Offensive Tactics

In the beginning of January 2016, a new German-language magazine was published – apparently by IS supporters – titled “Kybernetiq” (15 pp.) on Twitter and on Telegram channels. The magazine covers the topic of cyber warfare and emphasizes the great importance of learning cybernetic technology tools that will help jihadists win the battle against western countries as well as gain familiarity with applications and software to help achieve secure Internet use. For example, one article covered the encryption software “Asrar al-Mujahedeen” (“Mujahideen Secrets”), which is designed to enable secure dialogue between users. In addition, the editors of the magazine called for a translation of the articles into additional languages in order to increase the level of caution and alertness when surfing in cyberspace.

From left to right: an article regarding the importance of using encryption software such as "Asrar al-Mujahdeen"; the magazine banner

- The "Electronic Caliphate Army", which is affiliated with the Islamic State, published a link on its Telegram channel to an English guidebook titled, "Metasploit: The Penetration Tester's Guide" to teach beginner-level hacking using the Metasploit Project.



The guidebook banner

- On March 16, 2016 the "Al-Qaeda Electronic" hacking group claimed responsibility for the defacement of six Iranian Web sites.[8]

[8] March 16, 2016. https://dawaalhaq.com/

Review of Organizational Activities

The following is a summary of activities by hacker groups and individuals against various targets. Most of the hackers are involved in Web site defacement and the spread of political messages against regimes around the world. IS supporters continue to be active in cyberspace against a range of targets, including countries. In addition, other organizations such as Hezbollah and Hamas are also active in this arena. The offensive capability of these organizations is on the rise even though they do not currently have the ability to cause significant damage.

Islamic States Affiliates and Supporters

During this period, Islamic State affiliates and supporters continued to attack Web sites and social networks, and to leak information. An attempt by the organization was made to recruit Indian hackers for pay. This step illustrates how the organization is likely to quickly improve its offensive capability in cyberspace and cause more significant damage.

- At the end of January 2016, it was reported that IS members had offered to pay up to 10,000 dollars to hackers in India who successfully hacked into Indian government Web sites and stole sensitive information. This example indicates that the organization is attempting to recruit "mercenary hackers" who will take action in exchange for money, and not out of support for the organizations' activities.[9] According to an Indian expert in the field of cybercrime, approximately 30,000 young Indians made contact with IS members who offered payment amounts that had never been offered to local hackers. In December 2015, it was reported[10] that India intended to set up a war room for monitoring social networks 24 hours a day as part of its war against IS online activity in various regional Indian and Asian languages, in addition to Hindi and English.

- In the beginning of January, it was reported that IS operatives used the Facebook

[9] http://securityaffairs.co/wordpress/44019/hacking/isis-infiltrating-indian-hacking-community.html

[10] http://indiatoday.intoday.in/story/government-plans-social-media-scanning-centre-to-take-on-isis/1/554878.html

account of Ruqia Hassan Muhammed, an activist who acted against the organization. According to the report, IS fighters who killed the activist in September, claiming that she was a member of the Free Syrian Army, continued to operate her account on social networks with the goal of gathering information about additional opponents and journalists. This was part of the Islamic State's effort to obtain information from social networks in a variety of ways.[11]

- On January 18, it was reported[12] that hackers affiliated with the Islamic State had successfully defaced the Web site of Tsinghua University, one of China's leading universities that is involved in many research studies regarding national defense and security, and which serves as the "birthplace of information technology in China with the strongest technical teams in cyber security", as well as a target for online hacks by the NSA,[13] according to the Snowden documents. The defacement was signed "Islamic State Hacker". The university department responsible for Web site maintenance refused to confirm the incident but it immediately shut down the site once the breach was discovered. Nevertheless, the South China Morning Post reported[14] that a central member of the university's computer management team had confirmed to the newspaper that a breach was indeed carried out but he refused to provide additional details. A technical source at the university involved in the investigation into the incident stated that it is possible that a weak password was used for the university's Web site and that there is a low likelihood that IS hackers obtained advanced technology enabling them to breach the university's "firewall". He also stated that the university's Web sites were a frequent target for online attacks despite the statement that "the university's sites are considered to be better maintained and protected than many government sites in the country". However, it seems that this was the first time that hackers affiliated with the IS attacked a Web site

[11] https://www.hackread.com/isis-terrorists-kill-female-journalist-hack-facebook/
[12] http://www.scmp.com/news/china/policies-politics/article/1902268/islamic-state-hackers-attack-top-tier-chinese
[13] http://www.scmp.com/news/china/article/1266892/exclusive-nsa-targeted-chinas-tsinghua-university-extensive-hacking?page=all
[14] http://www.scmp.com/news/china/policies-politics/article/1902268/islamic-state-hackers-attack-top-tier-chinese

located in China. An announcement regarding the incident was also published[15] on the Facebook page of the CCTV Chinese television network.

Al-Qaeda in the Indian Subcontinent

In the beginning of February, it was reported that supporters of Al-Qaeda in the Indian Subcontinent had hacked and defaced a page on the Indian Railway's Web site, and posted a message to recruit the support of the Muslim population in India.[16] The 11-page English-language document titled, "Why is There No Storm in Your Ocean?", by Maulana Aasim, explains and justifies why jihad should take place in the Indian Subcontinent. [17] This incident emphasizes that the organization views railway infrastructure sites as a target for attack, including its Web sites.

Hezbollah

In February 2016, the existence of a Shi'ite hacker group affiliated with Hezbollah, named Kadimon (translation – We Are Coming), was reported in a television interview in Lebanon. The report raised the claim that members of the group had managed to hack into security cameras throughout Israel, including cameras in the Ministry of Defense at the government offices campus in Tel Aviv. It was also claimed that they had hacked into pages on social networks.[18] The belief is that a breach of security cameras is possible because it does not require advanced skill. Today one can find search services online that describe the IP address of IoT equipment, including cameras, around the world. In addition, it is worth remembering that in many cases, the end user does not change access passwords and leaves the default password, which is known and visible.

[15] https://www.facebook.com/cctvnewschina/photos/a.566725090034982.1073741828.565225540184937/1116471795060306/?type=3&theater
[16] http://www.bgr.in/news/al-qaeda-allegedly-hacks-indian-railway-website/
[17] http://www.satp.org/satporgtp/countries/India/document/papers/Wts.pdf
[18] http://www.timesofisrael.com/hezbollah-we-hacked-into-israeli-security-cameras/

Hamas

On March 22, a breach of @jpostdesk – one of the Jerusalem Post's Twitter accounts - was discovered when, starting at approximately 18:15, 16 messages were posted within less than 20 minutes in honor of the 12th anniversary of the assassination of Ahmed Yassin.

These included messages, photos and a link to a 01:22 minute long video containing Yassin's remarks against the Jews. Despite the fact that there was no official claim of responsibility, it is reasonable to assume that it was a Hamas supporter if not a member of the organization.

The messages, which were written in English and Hebrew, were designed to disseminate different messages; messages to the international community showing that the organization does not view them as a threat on the one hand, and messages threatening Israel on the other hand:

- Our main battle has always been against Israeli soldiers and Jewish settlers.
- The Zionists can thwart individual attacks but they cannot thwart an entire nation.
- Bus bombings are a legitimate act against the occupation.
- We will never recognize Israel because it is stealing our land and killing our children.
- We are not battling against the Americans or Europeans, we are only fighting against the Israeli enemy that took our homes and homeland from us.
- Choose this path and it will end with a martyr's death or victory.
- We do not want the occupation to end its hostile activities on our land, but rather we want it to leave our land.
- The Palestinian Nation has two choices: surrender or continue the resistance.
- We will not rest until we banish the last of the occupation from our land.

Cyber-Crime and Cyber-Terrorism, January-March 2016

Recent years have seen an increasing number of cyber-attacks on political targets, critical infrastructure, and the Web sites of commercial corporations. These attacks, which are also receiving increasing amounts of international attention, are perpetrated by states (which do not take responsibility for them), groups of hackers (such as Anonymous), criminal organizations and lone hackers. We believe that terrorist organizations are working in close collaboration with criminal organizations, are learning 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")[19] Internet between January - March 2016.

Major Cyber Incidents

- The London Police, in collaboration with the National Fraud Intelligence Bureau, published a document claiming that the damage caused by phishing scams throughout 2015 totalled 174.4 million pounds.[20] In addition, it was mentioned that there was a 21% rise in phishing frauds from 2014 in the UK. According to Symantec, spear-phishing against companies' employees increased by 55% during 2015, and attacks against small businesses with less than 250 employees have increased over the last five years.[21]
- According to a report by Arbor Networks, the most powerful DDoS attack in 2015 was at a volume of 500 Gpbs. This attack included a demand for a ransom payment in exchange for the termination of the attack.[22] The report mentioned that more service providers were ready to mitigate DDoS attacks in less than 20 minutes from 2013-2015.

These types of attacks continue to affect a range of sectors and infrastructure, and in some of the incidents the attacks manage to disrupt normal activity for hours.

On December 31, the BBC reported that its main Web site was subject to a DDoS online attack, which began at 07:00 GMT, which was confirmed in a press release:[23]

[19] 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.

[20] http://www.mirror.co.uk/news/uk-news/cyber-crime-soars-thousands-falling-7196796

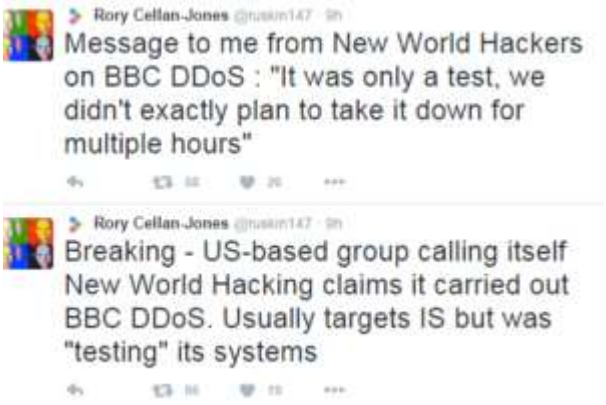
[21] https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf

[22] https://www.arbornetworks.com/insight-into-the-global-threat-landscape

[23] https://twitter.com/bbcpress/status/682490110034751488

Two-and-a-half hours later, another announcement was published,[24] according to which the Web site was back up and running:

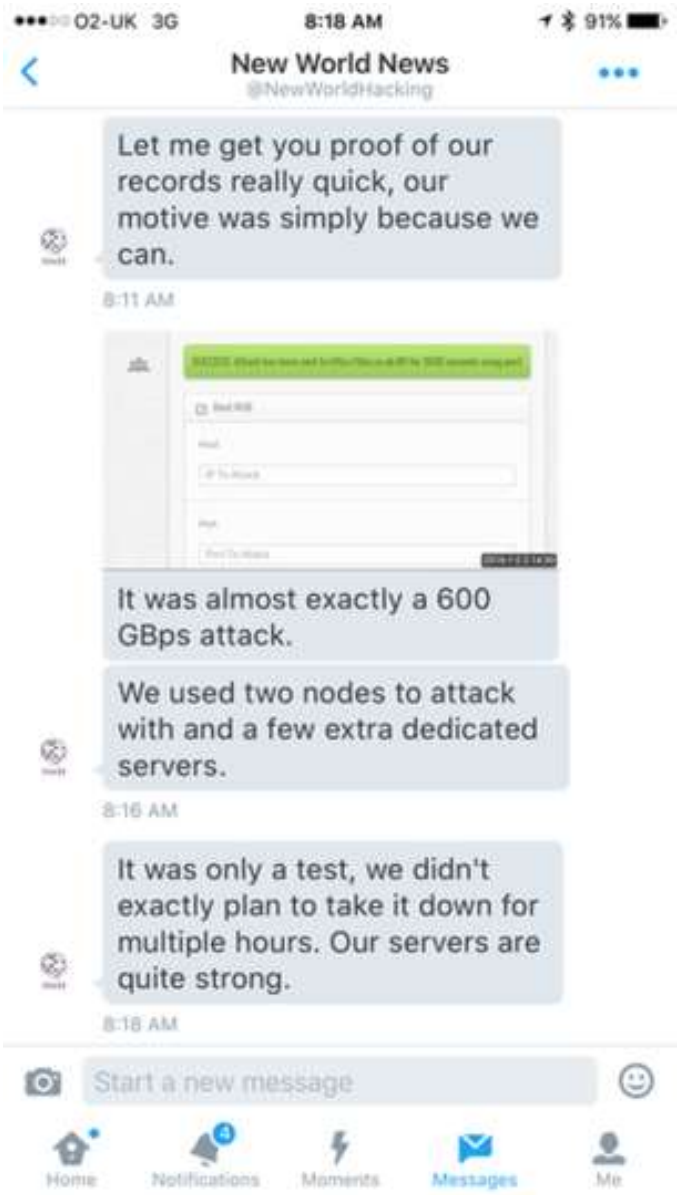
On January 2, another message was posted[25] on the BBC Web site, claiming that an organization named "New World Hacking" had claimed responsibility for the attack. According to the BBC, the organization acts against online activities tied to the Islamic State. A report about this incident was posted on two Twitter messages[26] that were posted by Rory Cellan-Jones, an economics and technology writer for the BBC, on his Twitter account:



In a message ascribed to the organization, it was claimed that it operates against the Islamic State, and that it did not intend to attack the BBC Web site but rather it was

[24] https://twitter.com/bbcpress/status/682528591184289792
[25] http://www.bbc.com/news/technology-35213415
[26] https://twitter.com/ruskin147

testing the organization's attack abilities and made a mistake.



DDoS is also affecting the financial system. In January, HSBC Bank in Britain was attacked twice and its online service was offline for several hours.[27]

[27] http://www.theregister.co.uk/2016/01/04/hsbc_says_sorry_for_online_banking_outage/

Screenshot from Twitter reporting on the second attack

It was later reported that the bank was cooperating with law enforcement authorities[28] in order to track down those responsible for the attack. It was also reported that the bank was continuing to protect its services[29] from the attack carried out on the same day, and that all of the bank's main branches would be open[30] the following Saturday. Two-and-a-half hours later it was reported that online and mobile banking services were in the process of being restored but the bank was still under DDos attacks.[31] Finally, after another four-and-a-half hours, a final announcement was posted according to which online and mobile banking services had been completely restored.[32]

- The Web site of the International Airport in Japan was attacked and disabled for four hours following a DDoS attack by a group associated with Anonymous. As part of the attack, the airport's official Web site was disrupted but no harm was caused to flight activity.[33]

[28] https://twitter.com/HSBC_UK/status/693053874618384386
[29] https://twitter.com/HSBC_UK/status/693075146672869376
[30] https://twitter.com/HSBC_UK/status/693075228092690436
[31] https://twitter.com/HSBC_UK/status/693112303533887488
[32] https://twitter.com/HSBC_UK/status/693178435116634113
[33] http://www.japantimes.co.jp/news/2016/01/23/national/narita-airport-website-hit-by-

- A Pakistani citizen, Muhammad Sohail Qasmani, who was wanted by the FBI, admitted to stealing and laundering millions of dollars as part of a hacking attack on a phone service (PBX). Qasmani worked with a group in Pakistan and Bangkok, which hacked the phone services of American companies and called premium call services (services which require paying a high fee). In this manner, the group fraudulently acquired about fifty thousand dollars. Qasmani laundered 19.6 million dollars, using 650 bank accounts in different countries.[34] It is important to note that similar methods have been used to fund terrorism.[35]
- On December 11, it was reported[36] that the Web site of the Danish Parliament[37] was shut down due to an online DDoS attack. A Parliament spokesperson confirmed that the attack began at 10:00 and stated that the government had no information regarding who or what group carried out the attack.
- The Ukrainian government decided to examine the level of preparedness for a cyber-attack targeting airports and critical infrastructure. This came after a successful cyber-attack using a malware named "BlackEnergy" was carried out in December 2015 and disrupted many services in the country, including electricity infrastructure, which affected 80,000 customers. In addition, it was published that the same malware was found in airport systems.[38]

Counter Measures

Following the terrorist attacks in Europe, it seems that European countries, in the framework of the European Union, are re-evaluating their battle against the Islamic State. In addition, in February, the launch of a US cyber campaign against the organization was reported, aimed at disrupting and even restricting its ability to operate on the Internet. It should be noted that cooperation between countries and

---

cyberattacks-possibly-linked-to-barring-of-the-cove-star/

[34] http://securityaffairs.co/wordpress/44476/cyber-crime/pbx-system-hacking-and-laundering.html

[35] http://www.infosecurity-magazine.com/news/four-people-arrested-in-connection-with-us/

[36] http://www.scmagazine.com/ddos-attack-knocks-danish-parliament-website-offline/article/459253/

[37] http://folketinget.dk/

[38] http://www.reuters.com/article/us-ukraine-cybersecurity-malware-idUSKCN0UW0R0

companies, such as Twitter, has been successful in removing IS content from the Internet.

- In the beginning of March, it was published that the United States had launched a cyber campaign against the IS aimed at disrupting and even preventing its online activity. According to US Secretary of Defense, Ash Cater: *"…interrupt [and] disrupt ISIL's command and control, to cause them to lose confidence in their networks, to overload their network so that they can't function, and do all of these things that will interrupt their ability to command and control forces there, control the population and the economy…"*[39] The assessment is that the US acted on several levels: attacking the organization's communications networks, using an algorithm for locating and removing content from the network, disrupting the communication frequencies used by the organization in areas under its control, and distributing content against the organization. It should be noted that during this period of time, several warnings were disseminated among IS members, including a warning that was distributed following the terrorist attack in Brussels in March 2016. The announcement contained instructions on using encrypted communication networks, encrypting files that are stored on the computer, using anonymous operating systems such as Tails, and avoiding revealing information on social networks.

[39] http://www.defense.gov/News/Transcripts/Transcript-View/Article/682341/department-of-defense-press-briefing-by-secretary-carter-and-gen-dunford-in-the

A screenshot from Telegram

- In the beginning of January, members of the CSU party in Germany presented a document that included recommendations to strengthen the war against terrorism. Among the recommendations was a reference to virtual coins, such as Bitcoin, addressing the need to monitor and track transactions as part of countering terrorism funding.[40]
- At the end of January 2016, as part of the hearings attended by European Union ministers, a new center for counter-terrorism established as part of Europol was presented. The center aims to improve the exchange of information between various law enforcement agencies, including information about online

[40] http://www.altcointoday.com/german-government-tracks-bitcoin/

activities.[41] The decision to establish the center was reached in March 2015, in addition to the Internet Referral Unit which began operating in June 2015. It is important to note that the terrorist attacks that have been carried out in European Union states over the last few years have brought about an organizational change in an attempt to improve counter-terrorism cooperation.

- The European Union's ENISA agency published a report summarizing the threats and dangers in cyberspace in 2015. The report ranks 15 threats, in which the top three are identical to those reported the previous year: namely, malware, Web-based attacks and web application attacks.[42]

  The report, which included an overview of threat agents, referred to cyber terrorists as part of IS activity in cyberspace. The report argued that the IS operates as a social online hacker (hackers who mainly operate on social networks and can carry out advanced social engineering attacks) and that the organization is trying to hire hackers to maintain their social activities. In conclusion, it mentioned that as there has been an increase in the availability of cyber-crime-as-a-service, through which the organization can improve its cyber capabilities. The report also mentions the contribution of hacktivist groups, such as Anonymous, in the effort to counter the activities of terrorists on the Internet.
- In the beginning of February, the US and the EU settled on a data and information sharing agreement between the countries, which will affect Facebook and Google. This agreement, termed a "Privacy Shield", will replace the "Safe Harbor" arrangement that has been used over the last 16 years.[43] The new agreement was formally adopted in July 2016.[44]
- Twitter announced that the company had suspended more than 125,000 accounts in the second half of 2015 for threatening or promoting terrorist acts.[45]

  The announcement mentioned that Twitter had increased the number of teams responsible for reviewing user reports in order to reduce the response time. In

[41] http://www.euractiv.com/section/justice-home-affairs/news/new-european-police-centre-launches-to-help-anti-terror-coordination/
[42] https://www.enisa.europa.eu/publications/etl2015
[43] http://www.securityweek.com/eu-us-agree-new-internet-privacy-shield
[44] http://europa.eu/rapid/press-release_IP-16-2461_en.htm
[45] https://blog.twitter.com/2016/combating-violent-extremism

addition, the teams searched for similar accounts with similar criteria or activities.

- The FBI requested more than $38 million to improve and develop capabilities to counter the threat of Going Dark, mainly by dealing with encrypted data and de-anonymizing users.[46]
- On November 30, Kazakhstan's telecommunication company published a press release[47] (which does not currently appear on the company's Web site), according to which as of January 1, 2016 a "national security certificate" will be enforced. According to the new law, "telecom operators are obliged to perform traffic pass with using protocols that support coding using security certificate, except traffic, coded by means of cryptographic information protection on the territory of the Republic of Kazakhstan. The national security certificate will secure protection of Kazakhstan users when using coded access protocols to foreign Internet resources".

  The company's Director of Innovation explained it as follows: "Internet users will be obliged to install the national security certificate, which will be available through the company's Internet resources. Users will have to enter the Web site and install the certificate according to the installation instructions, step-by-step." The installation will be available from any user device with an Internet connection, including mobile phones and laptops. He also stated that detailed installation instructions will be posted on the site during the month of December 2015. It should be noted that these are not the first governmental Internet restrictions in Kazakhstan, as others have been implemented in various forms over the last few years.

Ransomware

- Ransomware continues to pose a major threat from cybercrime organizations, and the trend of malware expansion continues to affect additional systems and devices, including Android mobile devices. In addition, there has been an

[46] http://securityaffairs.co/wordpress/44438/cyber-crime/fbi-38m-going-dark.html
[47] https://web.archive.org/web/20151202203337/http:/telecom.kz/en/news/view/18729

increase in the sale of ransomware-as-service, in which advanced malware can be purchased or downloaded to launch an independent attack.

- A new ransomware named "Lockdroid" was reported at the end of January. This ransomware can lock and erase data from Android devices.[48] In February it was reported that ransomware for OSX can be found on the Darknet and in underground forums.[49]
- Another type of ransomware, name "Magic", was built based upon an open-source ransomware that had been created for educational purposes.[50]
- The FBI's Internet Crime Complaint Center (IC3) reported that various ransomwares continue to spread and infect devices around the globe. IC3 stated that the known ransomware, CryptoWall, is the most significant threat targeting US individuals and businesses.[51] In addition, it was claimed that ransomware attacks were responsible for 42% of the security breaches in the UK in 2015.[52]

Case Study – "Killing Lists" – The Evolution of Cyber Terrorism?

Over the past year, there have been increasing calls warning of the possible danger of a successful cyber-attack by the Islamic State against the West. In the beginning of April 2016, Admiral Michael Rogers, Commander of the US Cyber Command, claimed that the IS could easily carry out cyber-attacks against the US.[53] The IS operates on the Internet as a platform for a very wide variety of uses but also views the space as an arena for battle. In the past, the organization carried out a number of successful cyber-attacks, including breaches of social network accounts as well as the theft and leak of information, such as lists containing the personal details of security forces.

It should be noted that it is difficult to identify and quantify terrorists who operate and carry out attacks in cyberspace since some of them operate under pseudonyms or aliases that change frequently. For instance, one of the first hackers to act on

[48] http://www.securityweek.com/lockdroid-ransomware-can-lock-smartphones-erase-data
[49] http://www.infosecisland.com/blogview/24699-OSX-Ransomware-Offered-for-Sale-in-the-Underground.html
[50] http://www.securityweek.com/new-magic-ransomware-based-open-source-code
[51] http://www.securityweek.com/its-official-ransomware-has-gone-corporate
[52] http://www.infosecurity-magazine.com/news/ransomware-42-uk-security-breaches/
[53] http://edition.cnn.com/2016/04/05/politics/isis-cyberattacks-michael-rogers/

behalf of the organization, and the one who was associated with it the most, was Junaid Hussain, a British hacker who was accused in Britain of hacking into the email accounts of Prime Minister Tony Blair. Hussain successfully evaded British authorities and arrived in Syria where he joined the IS and acted under the alias "Cyber Caliphate"[54] at a time when other hackers were also joining the IS. In April 2016, the IS announced the establishment of the United Cyber Army, which in composed of four different hacker groups that had previously operated separately: Caliphate Cyber Army, Sons Caliphate Army, Ghost Caliphate Section and Kalachnikv E-Security Team. It is difficult to assess the number of members in this organization.

A screenshot from Twitter

The new group raises concern of more sophisticated and complex cyber-attacks[55] due to, among other things, the fact that it threatens to act against the West. These threats are distributed mainly through posters or videos on Telegram channels or Twitter accounts.

Another type of action is the publication of "killing lists" that include personal information of individuals and calls for attacks on them. Back in March 2015, the

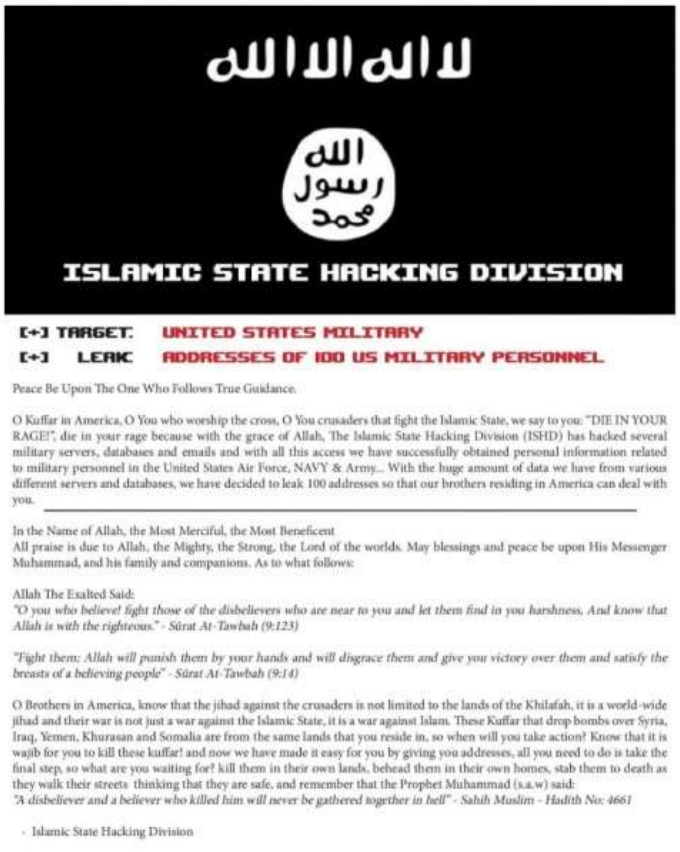
[54] http://www.ict.org.il/Article/1619/Cyber-Desk-Review-Report-14
[55] http://bgr.com/2016/04/28/isis-united-cyber-caliphate-hackers/

Islamic State Hacking Division (ISHD) and Cyber Chaliphat hacking groups published lists of US army personnel along with calls for attacks on them and threats against them and their families. The hacker groups claimed that they had managed to hack into US government and army databases and obtain details from them. Later, it was announced that a hacker named Ardit Ferizi had successfully hacked into the servers of a civilian company that held lists about American soldiers. After a failed extortion attempt, he contacted Junaid Hussain and sent him the lists.[56] Nevertheless, it should be noted that, according to the assessment, Hussain managed to hack into the Twitter account of US Central Command and, via this account, distributed the lists of soldiers, which increased the threat level and concern since it was a live account of a US Army authority.

[56] http://www.justice.gov/opa/pr/isil-linked-hacker-arrested-malaysia-us-charges

Screenshots from Twitter

The Islamic State Hacking Division group posted details including names, photos and addresses of army personnel. It seems that these details were taken from the Internet, including social networks or other public databases. The common assessment is that this was a smart intelligence move that included crossing information between various databases.



A screenshot from a document published by the Islamic State Hacking Division

It seems that in April 2016, longer killing lists were published that mainly included civilians. The lists were accompanied by an open call to "wolves" (the wording used in the publications) to attack the people who appear on the lists. For example, at the end of April a killing list was published that included approximately 3,600 people who are apparently New York City's elite.[57] These lists were distributed on various channels, including the Telegram application. According to some publications, the lists were also distributed through various Twitter accounts.

In June 2016, another list was distributed on Telegram that included the personal details of over 4,600 people. The list was accompanied by the following instruction: "Wolves of the Islamic State, a killing list is very important, kill them immediately, Caliphate Cyber Army, United Cyber Caliphate, Islamic State".

An examination of the contents of the list revealed that it was previously published (apparently at the beginning of 2014[58]) on the academia.edu Web site by a user named Arvind Yadav. According to the site on which it appeared, the list was viewed over 12,000 times. It seems that there is no connection between the person who posted the list to the Web site in 2014 and IS activists, and therefore it is reasonable to assume that the latter found the list on the Internet, and edited it to make it look like a new and original list.

A screenshot from Telegram

[57] http://www.mirror.co.uk/news/world-news/isis-hackers-release-hit-list-7864663
[58] https://web.archive.org/web/20140309073516/http://www.academia.edu/4371480/database_Arvind

This is a worrying trend because, unlike past lists, the current lists were published under the heading, "KILLIG LIST" and accompanied by a call on lone terrorists to take initiative and attack the people who appear on the list. Despite the difference between the types of lists, such as a list of army personnel versus a list of uninvolved civilians, it can be assumed that the call itself is designed to create panic among the public.

At the moment, it does not seem that the publication of these killing lists have achieved its goals since it has not created panic among the public or posed a real threat to human life. Nevertheless, it is unclear what the effect is among those people who appear on the lists and to what extent they are able to maintain their daily routine.

A screenshot of the list distributed by UCA

A screenshot of the original list[59]

[59] https://www.academia.edu/4371480/database_Arvind

ICT Cyber-Desk Team

Dr. Eitan Azani, Deputy Executive Director, ICT

Dr. Michael Barak, Team Research Manager, ICT

Dr. Tal Pavel, Expert on the Internet in the Middle East

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 Web sites 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.