Cyber-Terrorism Activities
Report No. 19
October - December 2016
Contents

Highlights ........................................................................................................................................... 3
Introduction ....................................................................................................................................... 4
Operational Usage by Jihadist Organizations .................................................................................. 5
Cyber Defensive Tactics ..................................................................................................................... 9
Offensive Tactics ............................................................................................................................... 16
Cyber-Crime and Cyber-Terrorism .................................................................................................... 19
Significant Incidents .......................................................................................................................... 19
Cyber Terror and Cybercrime Counter Measures .......................................................................... 21
**Highlights**

This report covers the period of October - December 2016, on 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).

During the period under review, terrorist organizations and their supporters continued to operate in the cyber world in similar ways as during the previous period. Nonetheless, it seems that recent emphasis was placed on the following:

- Considerable weight was given to the field of cyber protection, seemingly against the backdrop of increasing efforts by countries battling against terrorism to take the fight to the cyber world as well.

- The changes to the Islamic State’s situation in the physical world in general, and in Syria and Iraq in particular, influenced the scope and nature of the organization’s activity in the cyber world as well. For instance, the organization’s media institutions placed emphasis on the terrorist attacks that it carried out in Syria and Iraq – those allegedly carried out in the territory of the coalition countries fighting against the organization – and on encouraging lone wolf attacks in those countries. In our opinion, this type of propaganda is designed to overshadow the defeats suffered by the organization during the period under review, as well as the difficulties that it currently faces. Other terrorist organizations operated in a similar manner as they did in the past.

- The offensive cyber activity carried out by terrorist elements during the period under review mainly included Web site breaches and defacements, acts that reflect their technological capabilities. The offensive cyber activity carried out by criminal elements mainly included attacks for financial gain (including attacks to obtain ransom payment), most of which used platforms that were offered “for rent” by various hackers. It should be taken into account that activity carried out through rented platforms that enable an attack is liable to be adopted by terrorist organization as a means of funding their activities.
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 sites 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”, especially global terrorist organizations. However, such activity goes beyond the classic recipe of Internet use as a means of contact, recruitment, financing, publicity, incitement, psychological warfare and intelligence. Jihadist organizations are working on 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, and the media, and the main topics of jihadist discourse) and CYBER CRIME that is 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.

During the period under review, jihadist organizations continued to carry out propaganda activities with familiar features to the past.

- On November 8, 2016 a Telegram channel was launched under the name, “Market for Selling and Buying Weapons between Mujahideen Brothers”, which is linked to Syrian Salafi-jihadist rebels close to Jabhat Fateh al-Sham (formerly Al-Nusra Front, which was affiliated with Al-Qaeda). On this channel, a Czech pistol was offered for sale (at a price of $425), as were binoculars, silencers, bullet-proof vests and other military equipment.²

It should be noted that various communication channels, including Twitter accounts, involved in weapons trade in Syria were previously discovered.³

² https://t.me/soooooq
³ Read more: https://www.ict.org.il/Article/1937/the-bot-mujahideen-telegram-channel
The IS continued its propaganda efforts to present a picture of victory and steadfastness in the face of attacks by coalition forces. For instance, the Amaq news agency, which is involved in publicity for the organization, published an infographic about the scope of suicide attacks that IS fighters carried out in Iraq and Syria during the month of November 2016. According to this information, 132 fighters took part in suicide attacks (20 in Syria and 112 in Iraq) using 118 car bombs, nine explosive belts and five explosive vests. ^4

In addition to the above, the Amaq news agency also published an infographic about the attacks that IS fighters carried out in “coalition countries” [sic], first in France with 284 attacks (the length of time during which the attack took place was not noted). ^5

---

^4 5.12.16. https://jkikki.de/2016/12/05/132-
عملية-استشهادية-نفذها-مقاتلون-من-الد-132/  
The IS continued to use social networks to encourage lone wolf attacks in western countries. For example, the Yaqeen jihadist media institution, which is involved in publicity for the organization, published an infographic that included guidelines and suggestions for ways to carry out stabbing attacks.  

Bank al-Ansar, which belongs to the Afaq group that is involved in publicity for the IS, published an infographic on a Telegram account regarding the publicity assistance provided by IS supporters. According to this information, during October 2016, 5,994 accounts were handled by IS supporters, including 5,162 Twitter accounts, 732 Facebook accounts and 100 Telegram channels, and 50 fake telephone numbers were used. During November 2016, 7,250 accounts were handled by IS supporters, including 5,700 Twitter accounts, 1,100 Facebook accounts and 200 Telegram channels, and 250 fake telephone numbers were used.
The Afaq group, which is involved in publicity for the IS and publishes news regarding the cyber world, published an announcement on its Telegram channel regarding the launch of a Bot for the publication of the group’s video clips and texts.\(^7\)

On the “Bot Kuliyyat al-Mujahidin” (Bot Mujahideen College) Telegram channel, which has close ties to Salafi-jihadist fighters in Syria, including Jabhat Fateh al-Sham (previously Al-Nusra Front, which was identified with Al-Qaeda), it was published that two telegram channels – “Bot Mujahideen” and the “General Army Science Channel” – had merged due to “the urgent need to unite jihad efforts in the field of dawah and military training”.\(^8\)

**Cyber Defensive Tactics**

Terrorist organizations are aware of the tireless preventative efforts of security agencies and major players on the Internet in general, and on social networks in particular, to remove

---

\(^7\) Telegram.me/EHorizons

\(^8\) On the profile of the channel it states that the channel expressed a “unique military jihadist collective program on the Telegram social network, as it is not affiliated with any organization and adheres to the path of the Sunnah and jihad”. In addition, it states that “the Bot is a complete jihadist library. Its membership is composed of unique groups that are supervised by mujahideen and experts in their fields”.

@bot_mojahed2016_bot
jihadist content from their platforms. Therefore, these organizations continue to distribute defensive guidelines and instructions, and to expand their activities on the darknet where they claim to be better able to protect the traffic and anonymity of the organizations themselves, as well as their supporters, from the tracking software of intelligence agencies and activists who operate against terrorist organization on the Internet.

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

- The Afaq group, which is involved in publicity for the IS and publishes news regarding the cyber world, published on its Telegram channel a wide range of guidebooks on cyber-defense, including:
  - A link to a guidebook on VPN use.
  - A warning to users not to ignore or neglect safety rules while surfing the Internet.
    The publication highly recommended using VPN and Tor browser in order to hide the user’s online activity, and to preserve the anonymity and safety and the user.
    In addition, a video was published that was designed to raise users’ awareness of the issue based on leaks from US defense agencies and technological tools designed to track supporters of the Islamic State.
  - A warning to users against using VPN software that violates the privacy and security of users.
  - A recommendation to use the Web site, Virustotal.com, to check files and Web

---

9 Telegram.me/EHorizons.
10 These uses may enable the increased anonymity of the user. Today you can find a variety of VPN service providers for free or for payment.
sites for malware.

- An explanation regarding the use of the Qubes OS operating system, which improves the level of computer protection against breaches and tracking. Recommendations were previously published for using a similar system called Talis (see below).

![Qubes OS](image)

- A link to an explanation on how to install the Tor browser on the Linux mint 18 operating system.
- A link to an explanation about the Proxy Tor add-on to the Telegram application installed on the computer in order to hide user details.
- A link to an explanation about the use of ETHER software designed to install an operating system onto a portable device such as a USB or memory card. Using an operating system on a mobile device can protect the user against a physical search of the computer itself.

![ETHER](image)

- A link to a course on the topic of “computer security”, which included lessons on:
electronic security and fighting viruses on Windows and Mac systems; downloading and installing the Tor browser on the Windows, macOS and Linux operating systems; guarding against key logger; file encryption using vera crypt software; USB encryption and the removal of files; VPN services.

- A course on the topic of “Breaching Linux mint”, which included lessons on: downloading and installing the VERA CRYPT software for file encryption; downloading and installing the Linux system; downloading and removing the Linux mint software; installing the Tor browser on the Linux mint 18 operating system.

- A course on the topic of “Smartphone Security” (16 classes).

- A warning against the use of products by the Russian YANDEX company due to its cooperation with the Russian government and comparing it to the American Google, which violates the personal security of users and provides the government with identifying user data.

- An introduction to using the IsP network on Android, Windows and Linux
o An explanation regarding the ExifData software, which enables the editing and removal of meta-data, including GPS data, from photos on Android and iOS operating systems, in order to preserve the anonymity of the user.

o An explanation regarding the use of the F-Secure Freedom application, which is used for VPN services and protects anonymous data traffic. In addition, information was published regarding the PMP application, which enables management of access permissions to applications installed on a mobile device.

o A warning against using the fake Telegram channel of the Afaq group.

116.11.16. Also published on Twitter: https://justpaste.it/I2PNW
- An explanation regarding the use of a conversations applet and the operation of OMEMO Protocol on an encrypted network on Android devices.

- A link to a comprehensive guidebook on using Tails, an operating system that maintains user anonymity and works with TOR browser support.
- An article regarding encrypted e-mail services.

- An explanation regarding APK file scans on the Android operating system in order to ensure authenticity and absence of malware.

- An explanation regarding the use of Torrent, P2P software for transferring files.

- The re-publication of an old guidebook, which includes a course on computer security; a course on “the electronic security of smart phones”; an article regarding the downloading of files using torrent; videos, infographics regarding

---

12 First published on May 29, 2016. [https://justpaste.it/archivet](https://justpaste.it/archivet)
13 First published on February 20, 2016. [https://justpaste.it/PCsec](https://justpaste.it/PCsec)
14 First published on August 20, 2016. [https://justpaste.it/SMsec](https://justpaste.it/SMsec)
15 First published on June 18. [https://justpaste.it/TorrentD](https://justpaste.it/TorrentD), [https://justpaste.it/Tarticles](https://justpaste.it/Tarticles).
security and other topics.\textsuperscript{16}

\textbf{From left to right: an archive on various computer-related topics; a guidebook on electronic protection; a course of computer security}

- The “Bot Kuliyyat al-Mujahidin” Telegram channel, which has close ties to Salafi-jihadist fighters in Syria, including Jabhat Fateh al-Sham (previously Al-Nusra Front, which was identified with Al-Qaeda), published the following:\textsuperscript{17}
  - An audio clip by an anonymous spokesman warning members of the channel against taking pictures of jihad fighters in the battle arena and posting them on social networks.
  - A statement regarding the launch of several new Telegram channels that include courses on a wide range of topics, including electronic protection against hacking, Islamic law, air defense, armored vehicles and infantry.

**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

\textsuperscript{16} First published on February 20, 2016. https://justpaste.it/Secdgn
\textsuperscript{17} On the profile of the channel it states that the channel expresses a “unique military jihadist collective program on the Telegram social network, as it is not affiliated with any organization and adheres to the path of the Sunnah and jihad”. In addition, it states that “the Bot is a complete jihadist library. Its membership is composed of unique groups that are supervised by mujahideen and experts in their fields”. 
@bot_mojaheDe2016_bot.
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 offensive cyber tactics employed by terrorist organizations during the period under review included, among other incidents, the following:

- The United Cyber Caliphate, which is identified with the IS, claimed responsibility for the breach of the Facebook page and Telegram channel of “Raqqa is being Slaughtered Silently”, which collects news items regarding crimes carried out against the civilian population in Syria, especially by the IS. The site admitted that its Telegram channel had indeed been hacked.18

  From left to right: the Twitter account of “Raqqa is being Slaughtered Silently” acknowledging that its Telegram channel was closed due a hacking attack; a claim of responsibility for the attack

- The United Cyber Caliphate hacker group published a video titled, “They Want to Extinguish Allah’s Light with their Mouths”, which is drawn from a verse in the Quran. The spokesman of the group, Osed Agha, threatened that the group would continue to hack the Web sites and computer systems of the West, Shi’ites, Arab rulers and “their American masters”, and extract the names and residential addresses of individuals in order to enable lone wolves to assassinate them. In addition, he noted that new hackers, led by Cybrake, had joined the group.19

18 1.11.16. https://twitter.com/Raqqa_SL/status/793574178997825537?ref
19 26.12.16. https://www.youtube.com/watch?v=3OOefFL3wD0
The “Bot Kuliyyat al-Mujahidin” (Bot Mujahideen College) Telegram channel, which has close ties to Salafi-jihadist fighters in Syria, including Jabhat Fateh al-Sham (previously Al-Nusra Front, which was identified with Al-Qaeda), published an announcement according to which a hacker group called “The Electronic Jihad Army”, which belongs to the above-mentioned channel, had hacked and destroyed several Shi’ite Telegram channels in response to breaches, which were documented in several videos by Shi’ite elements such as “The Electronic Shi’ite Army”, that attempted to attack the Telegram channels of Sunni jihadist groups and their operatives.  

20

See also: [https://www.youtube.com/watch?v=sjMfe3QYzw](https://www.youtube.com/watch?v=sjMfe3QYzw) 13.11.16
Cyber-Crime and Cyber-Terrorism

Recent years have seen an increasing number of cyber-attacks against political targets, critical infrastructure, and the Web sites 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”) Internet between October - December 2016.

**Significant Incidents**

The cyber world continues to be an attractive focal point for attacks, both those aimed at obtaining information and demonstrating capabilities, and those aimed at making a financial profit. Among the many attacks that took place during the period under review were the following:

- In October 2016, the South Korean Ministry of Defense announced that the Army Cyber Command had been breached in September 2016. According to the information at our disposal, it seems that the hackers, possibly tied to North Korea, attacked a routing server that was installed in the Cyber Command, which was established in order to prevent breaches of the army’s computers. According to this information, on approximately 20,000 army computers are connected to the server, “hostile code was


22 [http://english.yonhapnews.co.kr/national/2016/10/01/82/0301000000AEN20161001001451315F.html](http://english.yonhapnews.co.kr/national/2016/10/01/82/0301000000AEN20161001001451315F.html)
detected that was apparently implanted under the cover of a weakness in the routing server”. The information also indicates that the army intranet is not connected to the server that was attacked and, therefore, the chances of classified information being leaked are low.

- The Director General of the International Atomic Energy Agency (IAEA), Yukiya Amano, warned that the threat of an attack on nuclear power plants should be taken seriously, and he added that a cyber-attack had taken place two or three years ago that caused the disruption of operations at a nuclear power plant, though not at a level that required the plant’s closure.23

- In November 2016 it was published that a 19-year-old man was arrested in Melbourne, Australia, on charges that between September 3 and November 5, he hacked the air traffic control system and broadcast 16 unauthorized transmissions to pilots on radio channels intended for airport officials, which led to disruption in the landing of one of those flights.24

- The San Francisco Municipal Railway (SFMTA), also known as the Muni, reported that the company’s network of ticket-selling machines had fallen victim to a ransomware attack in November 2016. The company did not charge its customers for their travel during the attack (until the systems recovery) and claimed that it would not meet the ransom demand for 100 bitcoin (approximately 73,000 dollars).25 According to the information at our disposal, the attack was apparently carried out by a hacker group called Cryptom27crew using the HDDCryptor ransomware, which is a platform for executing a RaaS (Ransomware As A Service) attack. It should be noted that, after realizing that they were not going to get the ransom payment due to restored system activity, the attackers claimed to have downloaded 30 GB of information from the company that they threatened to leak if they do not receive the ransom payment.26

In the beginning of December 2016, the Central Bank of Russia reported that hackers had managed to steal two billion rubles (approximately 31 million dollars) from the Central Bank and other banks after they faked customer bank information. According to the report, the hackers tried to steal five billion rubles but the bank managed to foil the attack and return some of the money.  

Cyber Terror and Cybercrime Counter Measures
Countries around the world continued to fight against cyber-crime and the various uses of the Internet employed by terrorist organizations. Among the noteworthy incidents are the following:

- Michael Fallon, the British Secretary of State for Defense, said in the framework of an international conference on advanced warfare systems in October 2016 that Britain had begun to attack the IS in cyber space. He added that Britain expects a significant cyber-attack at some point in the future and, therefore, is doubling its investments in the field of cyber defense to 1.9 billion pounds, out of which 256 million will be designated to search for security weaknesses in the army and critical cyber systems.

- American President-elect, Donald Trump, revealed in a speech that he gave on October 3, 2016 that his expected policy in the field of cyber security will be proactive and will include the launch of cyber offensive capabilities against states and terrorist organizations. Among other things, the President-elect stated that he would establish an international task force in the field of cyber security in order to combat hackers, and will consult with military commanders and other expert groups regarding ways to improve the nation’s cyber defense. The President-elect called on US agencies to act according to the “best and strongest” practices in the field of security, and to create new

---

ransomware/#7b72df9754dd
27 http://www.reuters.com/article/us-russia-cenbank-cyberattack-idUSKBN13R1TO
29 https://www.washingtonpost.com/video/politics/watch-trumps-speech-on-cyber-security/2016/10/03/06d2b1f6-897b-11e6-8cdc-4fbb1973b506_video.html
30 http://www.federaltimes.com/articles/trump-calls-for-crippling-cyber-attacks-on-us-enemies
training programs in this area for all employees as well as an offensive strategy that calls for strengthening the Cyber Command in accordance with the recommendation of the Joint Chiefs of Staff.

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

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.