IDC HERZLIYA

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

25 Report Cyber

2017 December

Cyber Report no. 25 by the International Institute for Counter-Terrorism (ICT) reviewed the prominent uses made of cyberspace by terrorist organizations and their supporters in December 2017. This is not an exhaustive list but rather an identification of the main trends as they arose from the field, and their analysis is divided into five areas.

1. In the operational domain, jihadist organizations continued to use cyberspace for a variety of needs, the most prominent among them being propaganda and financing. The dissemination of propaganda on social networks continued as usual during this period, while the financial aspect showed a drastic trend of the increased use of digital currency.
2. In the defensive domain of terrorists in cyberspace, there was no significant innovation. The trend of distributing content on issues of security and encryption, privacy and anonymity, warnings against phishing, and the safe use of mobile devices continued; most of the publications consisted of recycled content that was observed and documented over the past year, mainly through the Telegram channels of the "Electronic Afaq Horizons" institution.
3. domain offensive the In, the following stood out during the period under review: Caliphate Cyber Ghosts, which is associated with the Islamic State (IS) and hacker groups supported/directed by Iran. In addition, the third issue of the magazine, *Kybernetiq*, which is distributed by global jihad supporters and dedicated entirely to cyber-terrorism, was published. Terrorist organizations continued their efforts to improve their offensive capabilities, but they have not yet been fully developed.
4. In the domain between cyber-crime and cyber-terrorism, there was a trend of hacker groups operating under state direction – the main players being Russia, Iran and North Korea. While the attacks by Russia and Iran were aimed at espionage and intelligence gathering, North Korea launched cyber-attacks for economic gain. At the same time, there was an apparent trend of high-level data security risk stemming from the employment of subcontractors in critical projects/areas.
5. Coping with cyber-attacks, both crime-based and terrorism-based, requires global cooperation and out-of-the-box thinking. The countermeasures used are law and order, including regulation and prosecution for oversights/crimes occurring in the area, primarily for economic crime; setting a policy of refusing to negotiate with cyber-criminals; financing R&D projects of

technological solutions designed to make it harder for attackers; promoting cooperation between the private sector and the government sector.

Table of Contents

1. Uses perationalO

During the period under review, jihadist organizations continued to use cyberspace for a variety of operational needs, the most prominent among them being propaganda and financing. The content of the propaganda serves a double purpose; to sow fear (psychological warfare) and to serve as a catalyst for the execution of "lone wolf" attacks. The dissemination of propaganda on social networks continued as usual while the financial aspect, in contrast, gained tremendous momentum during this period.

Propaganda

The online propaganda mechanism of terrorist organizations continued to distribute content encouraging the execution of terrorist attacks. IS supporters customarily design banners that encourage attacks in accordance with current events, and during the period under review Christmas was presented as a set date to carry out attacks. The organization's official and unofficial media institutions produced psychological warfare videos alongside banners about the organization's media methodology. The following are examples of detected instances:

- During the month of December, IS supporters published a series of banners that contained threats to carry out attacks in crowded locations in the West, such as markets, malls, etc., against the backdrop of Christmas celebrations. Alongside this, threats to harm Jews were also published against the backdrop of Trump's declaration that Jerusalem is the capital of Israel (Telegram).

- The IS produced a video from Al-Hayat media institution containing a series of threats to carry out terrorist attacks on US soil. The messages in the video dealt with the following content: the Muslim Nation lived in the era of the Armageddon; the soldiers of the Caliphate may "sustain blows" here and there but they still remain strong; the terrorist who carried out the attack in Las Vegas converted to Islam and swore allegiance to the IS; Arab rulers are cooperating with the enemies of Islam.[1]

[1] http://www.dailymail.co.uk/news/article-5132459/ISIS-threatens-attacks-new-propaganda-video.html
http://www.dailymail.co.uk/news/article-5132459/ISIS-threatens-attacks-new-propaganda-video.html

Threats to carry out terrorist attacks in the West against the backdrop of Christmas celebrations

- The Fursan al-I'lam media group, which is involved in media for the IS, published a banner calling on anyone who wishes to assist in disseminating media for the organization to maintain the methodology that characterizes the organization and not to disseminate information that misrepresents the organization's path (Google Plus).

The banner of Fursan al-I'lam

Financing: Increasing Use of Digital Currency

The use of digital currency for the purpose of financing terrorism increased drastically during the period under review. Below are a series of documented instances of financing campaigns using digital currency that were identified during this period:[2]

[2] For the full report on the use of digital currency by jihadists, see: http://www.ict.org.il/images/Jihadists%20Use%20of%20Virtual%20Currency.pdf

- The Telegram account, "Technical Support for the Electronic Afaq Institution", a media group associated with the IS that focuses on the publication of materials concerning cyberspace, published a banner with a recommendation to make online purchases using the online currency, Zcash.

A recommendation for Zcash

- The Web site, Akhbar al-Muslimin which publishes news from the IS, launched an online fundraising campaign in November 2017. The site's administrators added a link to every media article that it published encouraging donations in the form of bitcoin virtual currency to help fund the site's operation, provided that the donation does not come zakat funds. A study that was published by the Intelligence and Terrorism Information Center in the beginning of December revealed that clicking on the link leads to a page designated for donation on the bitcoin trading site, coingate.[3] An independent examination conducted by the ICT Cyber Desk found that the diversion to coingate is no longer active; instead, the link diverts to an internal page on the site that was created on December 7, 2017, and any click on the link produces a different bitcoin address.

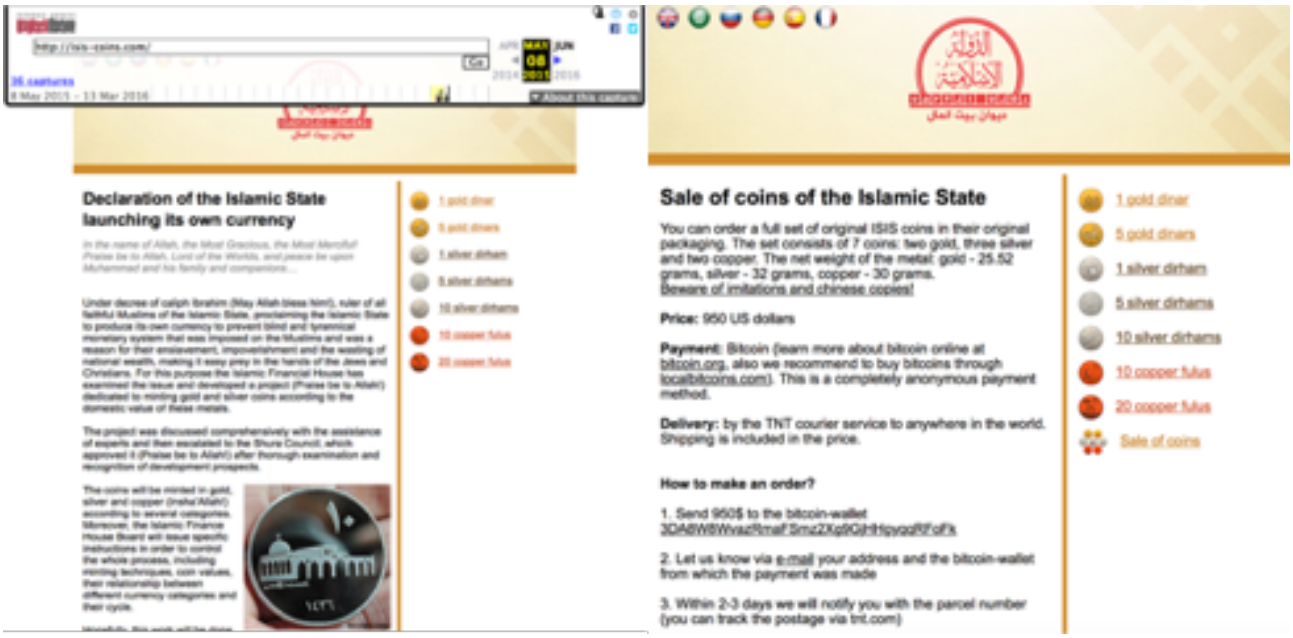
[3] http://www.terrorism-info.org.il/app/uploads/2017/12/H_235_17.pdf

Examples of various bitcoin wallets produced with every click on the fundraising link

- In December 2017, the Haqq site, which is affiliated with the IS, published an article about the sale of coins minted by the IS on a Web site.[4] In the summer of 2014, the IS declared the minting of local coins based on their intrinsic worth – gold, silver and copper. The launch of the new coin was published in *DABIQ* magazine and in a propaganda film titled, "Return of the Gold Dinar" (Al-Hayat). It was explained in these publications that the initiative is intended to keep IS supporters from using the Western banking system, which is based on a coin that is not made of precious metals, but rather is printed on paper notes and whose value is being manipulated by the central banks. The fall of the IS has made the coins redundant for conventional use as local currency in the territory of the Caliphate and they are apparently sold and exchanged as collectors' coins. The ICT Cyber Desk discovered a Web site called, "isis-coins.com" in which these coins are sold. The site is presented as an official site of the Islamic State's Finance Department containing the coins minted by the IS in accordance with the specifications described in the film titled, "Return of the Gold Dinar". Sets of seven coins are available for sale on the site: two gold coins, three silver coins, and two copper coins, at a cost of $950 per set and paid for using the virtual bitcoin currency. The site was registered in the Whois Registry on October 19, 2017 through a Russian brokerage firm (Moscow) that prevents the identification of the site's owners. However, there is evidence of discussion about this site in coin collectors' forums starting in 2015,[5] and we assume that the site was up and down periodically during this period. The 2015 version of the site, as saved in Web Archive, is missing the page that offers coins for sale. The credibility of the site was examined from various angles: the official symbol of the IS, the symbol of the Islamic State's Ministry of Finance (Bayt al-Mal), and from the linguistic- philological angle in the Arabic language. Although

[4] http://www.terrorism-info.org.il/app/uploads/2018/01/H_003_18.pdf
[5] https://en.numista.com/forum/topic37660.html

the findings revealed that these are authentic characteristics, it should be emphasized that it is impossible to confirm or refute the assumption that the IS is the owner of the site (documentation on the next page).



From left to right: a screenshot from the Web Archive site (May 8, 2015); a screenshot from the isis-coins.com site (January 17, 2018)

- Al-Sadaqah launched a fundraising campaign using digital currency. This is an independent organization that operates to assist the mujahideen in Syria, and supplies them with weapons, financial support and help with additional jihad-related projects.

Al-Sadaqah's campaign in Syria

2. The Defensive Domain

During the period under review, there was no significant innovation in the defensive domain of terrorists in cyberspace. The trend of distributing content on issues of security and encryption, privacy and anonymity, warnings against phishing and safe use of mobile devices continued; most of the publications consisted of recycled content that was observed and documented over the past year, mainly through the Telegram channels of the "Electronic Afaq Horizons" institution, a media group affiliated with the IS that focuses on the publication of materials concerning cyberspace. The following are several examples of the recycled content (source: Telegram):

- A guidebook on the use of the Kaspersky anti-virus software. The guidebook was provided in the framework of a course titled, "Computer Security Course: Electronic and Anti-Virus Protection". For example, it stated that the software allows the user to browse anonymously, prevents tracking, enables data encryption, and more.

A guidebook on how to use the Kaspersky anti-virus software

- A guidebook explaining the safe and secure use of Android devices.

A guidebook on safe use on Android devices

- An explanation about ransomware.

An explanation about ransomware

- A guidebook on how to use the Pidgin software, an encrypted chat software on the Windows operating system.

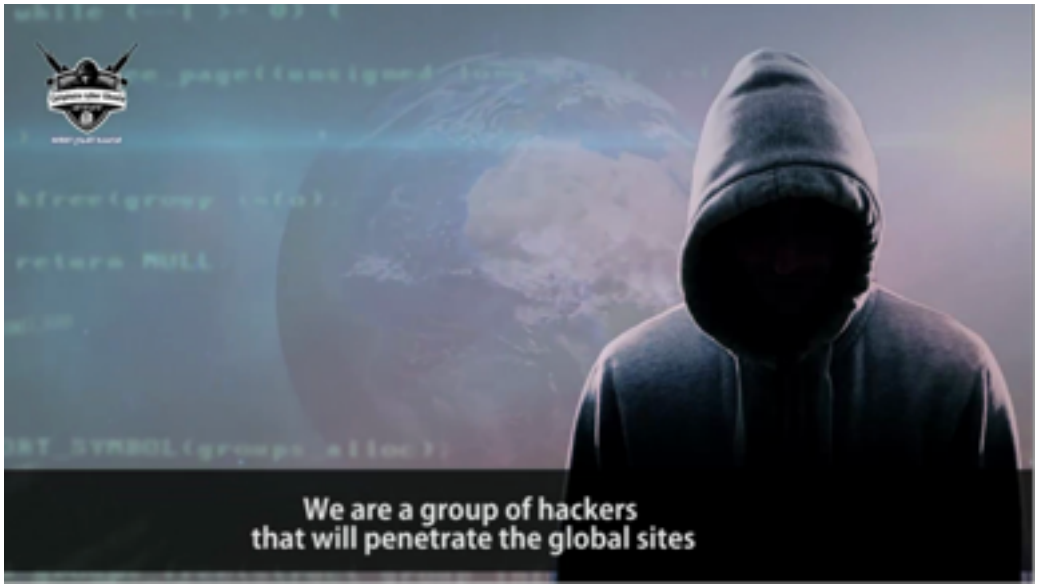
The Pidgin software

3. The Offensive Domain

Terrorist organizations continued their efforts to improve their offensive capabilities, but they have not yet been fully developed. However, it should be taken into account that these organizations may hire the services of hacker groups or acquire offensive capabilities with the assistance of terrorist-supporting countries. The following are hacker groups:

Hacker Groups

- An IS-supporting hacker group named Caliphate Cyber Ghosts published a video and several banners on its Telegram account threatening to launch an electronic attack on December 8 against all coalition countries participating in the war against the IS, especially against the US. The group claimed that its members had managed to penetrate classified Web sites of the US Army, Ministry of Interior, State Department and other offices, and to steal large amounts of classified material. The group added that it intended to publish some of the stolen information and to send the rest to lone terrorists in order to assassinate the individuals mentioned in the list and to intensify the scope of the attacks. In its concluding remarks, the group stressed that the IS would ultimately defeat its enemies. In another message, the same group announced that it had hacked into several US government and civilian Web sites during the second half of the month of December.



A screenshot from the Caliphate Cyber Ghosts' video

- Iran is strengthening its cyber warfare program. Iran is one of the leading cyber rivals of the US. It developed its program only a few years after Russia and China, and so far, has demonstrated less ability than the latter. Nevertheless, Iran has carried out several cyber-attacks that caused a great deal of damage, and has become a fundamental threat that will develop and grow. Like Russia and China but unlike other countries, Iran openly encourages its hackers to attack its

enemies. Thus, the country not only recruits hackers to its ranks but even encourages independent attacks (December 12, 2017).[6]

Digital Magazines

Digital magazines serve as an effective tool for transmitting information in a modern communication channel (not through television/radio). Most of the magazines published by terrorist organizations carry propaganda messages, such as *INSPIRE, DABIQ* and *Rumiyah*; Several (three) issues of the magazine, *Kybernetiq*, which is dedicated entirely to cyber-terrorism, were published:

- The third issue of the cyber warfare magazine *Kybernetiq*, was published. *Kybernetiq* is a German-language digital magazine that covers cyber warfare. The magazine is directly associated with global jihad supporters and, contrary to popular perception, it cannot be unequivocally determined that it is associated with the IS. Three issues of the magazine were published at intervals of about one year from each other. The third issue was designed at a high level and it is clear that it appeals to a Western audience - both in light of the choice of the writing language and the use of pop culture as a recurring graphic motif. Each issue opens with a preface that relates to Western media and ends with a Sci-Fi style story. The main chapters deal with analyses of organized cyber-attacks, a discussion of programming languages, attack tools, Pen-Tests, digital forensics, botnets, how to cope with the challenges of computerization by the German intelligence, and recommendations for technological solutions for privacy protection in cyber-space. The magazine can be downloaded from a dedicated site that is accessible via TOR (onion domain suffix).

Issue no. 3 of *Kybernetiq*

[6] http://www.newsweek.com/irans-cyber-warfare-program-now-major-threat-united-states-745427

4. Cyber-Crime and Cyber-Terrorism

In recent years, cyber-attacks have been used for political purposes. These attacks, which are carried out by hacker groups, are actually directed by countries that benefit from the difficulty in (legally) attributing the attack to the group. Terrorist organizations develop and learn from these attacks and may even hire the services of the hackers. Therefore, it is important to examine and analyze the line that falls between crime and terrorism in cyberspace.

Attacks Directed by States

During the period under review, there was a prominent trend of hacker groups operating under state direction and attacking political targets. The main players were Russia, Iran and North Korea. While the attacks by Russia and Iran were aimed at espionage and intelligence gathering, North Korea launched cyber-attacks for economic gain. The following are state-directed cyber-attacks that were identified during the period under review:

- The Russian hacker group, Fancy Bear, carried out a cyber-attack against journalistic targets and media personnel that regularly published content hostile to the Kremlin. The goal of the attack was spying, and in that framework the group hacked into the Gmail accounts of at least 200 journalists and bloggers on the Internet, starting in mid-2014. Appearing on the list of the group's targets were American, Russian and Ukrainian, and eastern European media personnel. The list of targets is evidence of the conclusion made by the American intelligence community that Fancy Bear acted (favorably) in the service of the Russian government when it intervened in the American presidential elections; the Kremlin denies the accusations (December 22, 2017).[7]

- The company, FireEye, identified an espionage attack against a government organization in the Middle East. The company estimates that the attack was carried out by the Iranian hacker group, APT34, which is involved in a long-range cyber espionage operation that focuses primarily on intelligence gathering efforts in Iran's interests; it has operated since at least 2014. This group carried out extensive attacks against a variety of sectors, including governments and the energy, chemical and communications industries, and has focused its activities on the Middle East. It is

[7] https://www.usatoday.com/story/news/world/2017/12/22/election-hackers-pursued-reporters-russia-united-states/975920001/
http://abcnews.go.com/International/wireStory/russian-hackers-targeted-200-journalists-globally-51948081
https://nypost.com/2017/12/22/russian-hackers-targeted-hundreds-of-journalists-around-the-world/
https://www.apnews.com/c3b26c647e794073b7626befa146caad

estimated that APT34 operates under the direction of the Iranian government based on infrastructure details that include references to Iran, the use of Iranian infrastructure, and the choice of targets that are compatible with the interests of the nation-state. The APT34 group uses a mix of public and non-public tools, and often carries out phishing operations through hacked accounts, sometimes combined with social engineering tactics (December 7, 2017).[8]

- The cryptographic currency trading platform, YouBit (formerly Yapizon), filed a request for bankruptcy after it again fell victim to hacking by cyber criminals. The breach wiped out approximately 17% of its assets. In April 2017, the South Korean platform suffered a breach in the framework of which approximately 4,000 bitcoin were stolen. As a result of the breach, an investigation was launched by the country's intelligence services for fear of North Korean involvement aimed at increasing the state coffers by means of cryptographic currency (December 20, 2017).[9]

- The White House formally accused North Korea of launching the "WannaCry" ransomware attack that took place in May 2017. The ransomware disrupted the activities of hospitals, banks and commercial companies around the world. The US is not the only country to have reached the conclusion that the attack was carried out by North Korea; Britain and Microsoft reached similar conclusions in independent analyses carried out after the attack. The North Korean Foreign Ministry denied the allegations (December 17, 2017).[10]

[8] https://www.infosecurity-magazine.com/news/iranian-blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html
https://www.infosecurity-magazine.com/news/iranian-statesponsored-apt-34/
https://www.wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/
https://www.reuters.com/article/us-far-eastern-fine/taiwans-far-eastern-international-fined-t8-million-over-swift-hacking-incident-idUSKBN1E60Y3

[9] https://bitcoinist.com/youbit-bankruptcy-hackers-assets/ https://cryptovest.com/news/another-bitcoin-exchange-hacked-youbit-files-bankruptcy-after-losing-users-coins/ https://themerkle.com/youbit-hacked-again-closes-its-doors/

[10] https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537
https://www.reuters.com/article/us-northkorea-missiles-cyber/north-korea-rejects-u-s-accusation-says-it-is-not-linked-to-any-cyber-attacks-idUSKBN1EF0BD
https://www.cbsnews.com/news/north-korea-wannacry-cyberattack-tom-bossert-oped/
http://edition.cnn.com/2017/12/18/politics/white-house-tom-bossert-north-korea-wannacry/index.html
https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q

Point of Vulnerability: Subcontractors

The NSA has a history of information leaks (and attack tools) carried out by subcontractors, the most famous of which was the case of Edward Snowden. The following is a list of similar incidents that expose the risk posed to information security resulting from the use of subcontractors:

- Le Duc Hoang Hai, 31, a Vietnamese hacker, hacked into the computer system of Perth Airport and stole sensitive data about aviation infrastructure and security in Perth Airport. The incident took place in March 2016 when the hacker obtained entry permits to the systems of a third-party contractor that allowed him access to the aviation systems. Hai stole significant amounts of data concerning the airport, including sketches and details regarding physical security in the airport's buildings. However, there was no breach of radar or other aircraft takeoff and landing systems, so passengers were not at risk. An investigation of the breach led to Vietnam and the Australian Federal Police activated its colleagues in Vietnam to arrest Hai. He was sentenced to four years in prison. In addition to the breach of Perth Airport, it was discovered that Hai had attacked infrastructure and Web sites in Vietnam, including those of banks, telecommunication and an online military newspaper (December 11, 2017).[11]

- The head of the German intelligence agency, BfV, warned that Chinese cyber spies are using social networks to attack European entities. According to him, it is a large-scale attempt to infiltrate parliaments, government ministries and government agencies. The German intelligence agency reported that over 10,000 Germans were targets for Chinese intelligence agents who posed as consultants, headhunters (in the field of placement) or researchers, especially on the networking site, LinkedIn. It also reported that Chinese hackers are investing in attacks against European companies through trusted suppliers and through "supply chain" attacks designed to circumvent corporate protections. Such attacks are directed against IT workers and other employees who serve as trusted service providers, and enable malicious software to be sent through them to networks of organizations that the attackers want to attack (December 10, 2017).[12]

[11] http://www.ibtimes.co.uk/perth-airport-hack-vietnamese-hacker-steals-significant-amount-security-data-building-plans-1650933
http://www.computerweekly.com/news/450431587/Perth-airport-security-plans-stolen-by-Vietnamese-hacker
http://www.dailymail.co.uk/news/article-5165727/Hacker-Vietnam-stole-security-data-Perth-Airport.html
https://thewest.com.au/news/wa/significant-amount-of-sensitive-security-data-stolen-in-perth-airport-hacking-ng-b88686393z

[12] http://www.bbc.com/news/world-europe-42304297

5. Coping

Coping with cyber-attacks, both crime-based and terrorism-based, requires global cooperation and out-of-the-box thinking. New tools (attack tools) require new laws. The following are descriptions of countermeasures used by global players to eradicate the phenomenon of cyber-attacks:

Law, Order and Regulation

The law crystallizes out of a need that arises in a particular society to which it provides an answer. Therefore, the law often tends to be formulated late in relation to the date of the incident. The legal battle against cyber-attacks may be based on the introduction of "ordinary" laws on cyberspace and, alternatively, on specific legislation tailored to the details of an attack in cyberspace, which of course requires prior preparation. Below is a list of several cases demonstrating coping methods that were used during the period under review:

- Taiwan's financial regulator fined the Far Eastern International Bank $266,524 as a result of deficiencies related to the breach of its SWIFT system. In October 2017, Taiwan's local media reported that hackers had stolen approximately 60 million dollars from the bank and that all of the money, with the exception of $500,000, was returned by the bank. The bank's own investigation as well as the investigation by the regulator, revealed that in this incident the information security system was not fully prepared, the account was not adequately managed, and the bank did not reinforce its SWIFT security system. For these reasons and others, the regulator noted that the bank did not secure its internal control system for information security and, as a result, violated a clause in Taiwan's banking law. The regulator also stated that it would work to improve its regulatory system in connection with information security, including inviting external experts to participate.[13]

- The Federal Court in Central Islip, New York, filed an indictment against Zoobia Shahnaz from Long Island for bank fraud and money laundering for the purpose of supporting terrorism (December 14, 2017). The defendant was suspected of defrauding several financial entities, stealing and

https://www.ft.com/content/31c2884e-ddc8-11e7-a8a4-0a1e63a52f9c http://www.dailymail.co.uk/news/article-5164365/German-intelligence-warns-increased-Chinese-cyberspying.html https://mobile.nytimes.com/aponline/2017/12/10/world/europe/ap-eu-germany-china-spying.html?partner=IFTTT&referer=https://t.co/S4R4Q7ERId?amp=1

[13] http://focustaiwan.tw/news/aeco/201712120025.aspx http://ktwb.com/news/articles/2017/dec/12/taiwans-far-eastern-intl-fined-t8-million-over-swift-hacking-incident/?platform=hootsuite https://www.fireeye.com/

laundering over $85,000 of illegal returns using Bitcoin digital currency and other digital currencies between March and July 2017. The funds were transferred out of the country to straw entities in Pakistan, China and Turkey, and were intended to support the IS. The defendant attempted to flee the US to Syria and was arrested by the authorities after questioning in JFK.[14]

Non-Surrender Policy

One of the most prominent cyberspace threats in recent times is the ransomware attack. This attack is extremely attractive to terrorist elements because of the duality that it offers - both the execution of electronic jihad and a means of financing. Similar to physical ransom (or hostage) scenarios, an online scenario requires the delineation of a clear response policy similar to that used in North Carolina. Below are the details of the case:

- Mecklenburg County, North Carolina, United States, refused to pay hackers a ransom in the amount of $23,000 in exchange for the release of information held in the county's computer system, which had been hacked. The hackers, who appear to have operated from Iran or Ukraine, froze the site and the other electronic services of Mecklenburg County, and demanded a ransom to restore the situation to its former state. The country decided not to surrender to the hackers' demands. In view of the decision, the country will now use available backup data to rebuild its system, giving priority to the departments that influence the court, health and social services, and environmental services.[15]

Inter-Sectoral Cooperation

Counterterrorism and cyber threats share a common characteristic - both require broad cooperation. Cooperation can be between countries, between organizations and even cross-sectoral. The following are relevant collaborations that took place during the period under review:

- ESET's security researchers, in cooperation with Microsoft, law enforcement agencies, the FBI, Interpol, Europol and other information security agencies, took part in a major campaign to topple a botnet known as Andromeda, which has been infecting victims since 2011. Cooperation between the entities began on November 29, 2017, and as a result of the joint effort law

[14] https://www.justice.gov/usao-edny/pr/long-island-woman-indicted-bank-fraud-and-money-laundering-support-terrorists

[15] http://www.hickoryrecord.com/news/state/north-carolina-county-won-t-pay-hacker-ransom/article_5efc9665-28cb-5c60-b564-9f10a8f039b9.html http://www.wbtv.com/story/37007041/county-computer-hackers-demanding-substantially-more-than-first-reported http://abcnews.go.com/US/wireStory/latest-carolina-sheriff-affected-county-hacking-51617202

enforcement agencies around the world were able to carry out an arrest and block the activities of a family of malware responsible for infecting 1.1 million systems a day and which distributed, among other things, the known ransomware, Petya and Cerber. Microsoft and ESET investigators shared technical analyses, statistical information and the domain addresses and Command and Control servers in order to help disrupt the malicious activity of the group. Over the last year-and-a-half, ESET also shared information about Andromeda that was obtained from the constant monitoring of malware and botnet networks. In addition, law enforcement authorities in Belarus arrested a suspect in the creation of Andromeda's malicious code, which would not have been possible without the information provided to them. During the first 48 hours following the seizure of the command and control servers by the authorities, it was discovered that the network was currently spread out over 223 countries, with more than 2 million infected computers attempting to connect to it.[16]

- Eugene Kaspersky, the founder of the security company bearing his name (Kaspersky Lab), made it clear that he would leave Russia if its intelligence services would ever ask his company to spy for it. According to Kaspersky, if the Russian government would ask him and ask him or his employees to do something improper, he would take his business out of Russia since his company never helped spy agencies, Russians or any other country. Kaspersky mentioned that the company's products were designed to stop attacks and identify malicious code, not to spy on the company's customers. The statements of the Russian information security giant came on the heels of the findings of an investigation that it presented in November 2017, which contradicts claims of the company's involvement in Russian espionage in the United States.[17]

Solutions Technological R&D

- DARPA (The Defense Advanced Research Projects Agency of the US Department of Defense) awarded a grant in the amount of $3.6M to a team from the University of Michigan to fund the technological development of an un-hackable computer. The name of the project is Morpheus and the software is intended to present a new way to design hardware so that information passes

[16] https://www.reuters.com/article/us-cybercrime-botnet-belarus/belarus-arrests-suspected-ringleader-of-global-cyber-crime-network-idUSKBN1DZ1VY
https://blogs.technet.microsoft.com/mmpc/2017/12/04/microsoft-teams-up-with-law-enforcement-and-other-partners-to-disrupt-gamarue-andromeda/

[17] https://www.theguardian.com/technology/2017/nov/30/eugene-kaspersky-russian-spies-us-government- http://www.zdnet.com/article/eugene-kaspersky-we-would-quit-moscow-if-russia-asked-us-to-spy/

quickly and randomly, and is then destroyed. The goal of the technology is to make it harder for attackers to get the critical information they need to build a successful attack, and to protect hardware and software.[18]

[18] https://www.digitaltrends.com/computing/darpa-u-michigan-morpheus-unhackable-computer/ https://www.extremetech.com/extreme/261052-darpa-university-michigan-team-build-unhackable-chip https://news.engin.umich.edu/2017/12/unhackable-computer-under-development-with-3-6m-darpa-grant/

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

CYBER-DESK TEAM

ICT Director, Executive Deputy Azani, Eitan Dr.

Dr. Michael Barak, Team Research Manager, ICT

ICT Researcher, Senior Yaakov, Ben Uri Adv.

Nadine Liv, Researcher, ICT

CYBER-DESK CONTRIBUTORS

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

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

Oren Elimelech, Cyber Security Expert, Researcher & Consultant

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

Dr. Menashri Harel, Research Fellow, ICT, & Cyber, Information Security & Technological Intelligence Expert, Israel

Nir Tordjman, Research fellow, ICT

The research was facilitated by a special technology for the collection and analysis of information gathered from the DarkNet, developed by Athena from Mer Group in cooperation with SixGill.