IDC HERZLIYA

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

ICT Cyber-Desk

PERIODIC REVIEW

Cyber-Terrorism Activities

Report No. 12

January – March 2015

Highlights

This report covers the period of January - March 2015 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:

- During January-March 2015, a prominent activist calling himself "The Islamic State's Technology Expert", and who is affiliated with the Islamic State (IS) on social networks, published several guidebooks and precautions on topics including, how to operate securely and secretly on social networks, how to maintain anonymity and encryption of cellular devices, how to use TOR technology on various devices form desktops to laptops, how to secure and encrypt information on personal computers, etc.
- Since the beginning of 2015 there has been in increase in cyberattacks by elements affiliated with the IS, including the defacement of Web sites and Twitter accounts, as well as information leaks. The attacks were carried out by various groups using the organization's logo, such as the CyberCaliphate, or by parties acting on behalf of the organization, such as the Islamic State Hacking Division.
- The terrorist attack against the French magazine, *Charlie Hebdo*, in Paris led to mutual cyber-attacks with supporters of the IS attacking various targets, mainly in France. On the other hand, members of 'Anonymous' increased the fight against the IS and acted to disrupt activities on forums and Internet sites affiliated with the organization. In addition, as part of the OPISIS campaign, Twitter accounts of IS members were identified and blocked.
- During January-March 2015, trading in the amount of approximately 4.5 million bitcoins – worth over one billion dollars - took place on the Bitfinex site. At the start of the year, the average value of the currency stood at approximately 320 dollars and by the end of March its value had dropped to 245 dollars. Trading sites continued to serve as targets for cyber criminals, and several other sites were hacked and millions of dollars' worth of coins were stolen.
- The United Nations Security Council stepped up its efforts to engage Member States in a variety of measures to combat terrorism over the past few months, in particular to mitigate the increased use of cyberspace by extremist groups in the Middle East. Three resolutions in particular exemplify this new approach, noted under the category of "Threats to peace and

security caused by terrorist acts" and prompted by acts of terrorism and their promotion via the internet by the IS, ANF, Al-Qaeda and similar terrorist groups.

- This report includes an analysis of #OpIsrael 2015. This attack repeats itself on the same date every year with minor changes – each year different attack techniques are used, and the security response of organizations in Israel vary as do the results of the attack. The history of this series of attacks reflects the changes and changing trends of cyberattacks over the years, and the evolution of the security actions taken against them.

Table of Contents

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 2015[1]

The Rift between Al-Qaeda and the Islamic State

The rift between Al-Qaeda and the Islamic State (IS) continued to occupy a significant part of the jihadist discourse and was characterized by mutual bickering and war narratives. For example, Ali Abu Muhammad al-Daghistani, Emir of the Islamic Caucasus Emirate, issued a scathing criticism of the IS and its leader, Abu Bakr al-Baghdadi, and accused them of trying to sow division among the ranks of the mujahideen in the Caucasus. According to him, jihad fighters in the Caucasus who swore allegiance to al-Baghdadi did so out of ignorance and a lack of knowledge of shari'a, and this trend should cease immediately. On the other hand, the IS continued its attempts to recruit other fighters from various areas to its ranks. For instance, it appealed to the Berberb population in Libya, Algeria and northern Mali to join its ranks and swear allegiance to its leader, al-Baghdadi.

Another sign of the rift could be seen in the oaths of allegiance taken by various jihadists and jihad organizations to the IS. In Pakistan and Afghanistan, approximately ten jihadist groups swore allegiance to al-Baghdadi, the leader of the Islamic Caliphate, and declared the establishment of a new province in the region called Khorasan. Abu Muhammad al-Adnani, the spokesman for the IS, announced the establishment of the new province in response to the expansion of the IS to this

[1] For a more thorough review of jihadist life on the Web, see the ICT's Jihadi Website Monitoring Group's Periodic reports, at http://www.ict.org.il/ContentWorld.aspx?ID=21

area.

The West

The terrorist attacks against the French magazine, Charlie Hebdo, in the jihadist discourse

The terrorist attacks carried out by the Kouachi brothers - Muslims French citizens of Algerian origin - against the French satirical magazine, *Charlie Hebdo*, in Paris, as well as the attack carried out by their friend, Amedy Coulibaly – a French citizen from Mali – at a Jewish supermarket in Paris occupied a significant part of the jihadist discourse during January-February.

Al-Qaeda in the Arabian Peninsula (AQAP) claimed responsibility for the attack at the French satirical magazine, *Charlie Hebdo*, in Paris and explained that it was carried out in revenge for disrespecting the Prophet Muhammad, who was mocked in a caricature. Many jihadists and organizations, including Al-Qaeda in the Islamic Maghreb (AQIM) and the IS, blessed the attack, justified it and called on Muslims in the West, and especially those in France, to continue the wave of attacks. Nasser bin Ali al-Ansi, a senior member of AQAP, also called on Muslims in the West, and especially those in France, to adopt the "lone wolf" type of attack that was used in Paris. Sheikh Ibrahim al-Rubaysh, a member of AQAP's Shura Council, declared that France would pay a heavy price in its security and economy, and emphasized that it should be considered the first target for attacks. Al-Shabab Al-Mujahideen, Al-Qaeda's branch in Somalia, also threatened that French civilians would not enjoy personal security and would experience similar attacks should it continue to act against Islam and to insult the Prophet Muhammad.

The IS also "rode the wave" of sympathy sparked by the attacks, and flooded its PR system with praise for individual terrorist attacks against European countries, especially France. In addition to this development, Al-Shabab Al-Mujahideen called on "lone wolves" to attack commercial shopping centers, such as malls, in Canada, the United States and Britain.

Campaign against coalition forces' attacks in Iraq and Syria

As part of the Islamic State's psychological warfare against the coalition forces fighting against the organization in Iraq and Syria, the IS made several threats to execute two Japanese captives in response to the Japanese government's promise to transfer 200 million dollars to the coalition forces fighting against the organization. However, it expressed a willingness to spare the lives of the two hostages on the condition that the Japanese government send a similar amount to the IS. After it executed one of the hostages, the IS demanded the release of the female terrorist, Sajida al-Rishawi, from prison in exchange for the release of the second Japanese hostage. In the end, the IS followed through on its threat and executed the hostage.

Documentation of the execution of the Jordanian pilot who was captured by the IS at the end of December 2014 and burned to death in a cage also occupied a prominent place in the jihadist discourse during the month of February. IS members justified the manner in which he was executed, claiming that it was an equivalent retaliation for the burning of Muslim residents by coalition aircraft fire. In addition, the IS threatened that should Jordan execute the terrorist, al-Rishawi, in revenge for the death of the Jordanian pilot, the IS would begin a wave of attacks against the Jordanian Kingdom. In the framework of the Islamic State's propaganda war and increased warnings not to take part in air strikes against the organization, the organization published an official list of the names of Jordanian pilots and their addresses as potential targets for assassination.

Yemen

The Killing of Sheikh Harith al-Nathari

The killing of Sheikh Harith al-Nathari, a member of AQAP's Shura Council, in an American drone strike also occupied the jihadist discourse for a long time. The organization accused the Houthi Shi'ite minority in Yemen of bearing responsibility for the killing as a result of its cooperation with American forces. Many jihadist organizations, including Al-Qaeda's affiliates, published eulogies in his memory and some of them called for revenge attacks to be carried out against American targets.

Egypt

Ajnad Misr, a Salafi-jihadist organization operating in Egypt, called on Muslims to concentrate their efforts on attacks against Egyptian security forces as a necessary step in applying shari'a in Egypt. According to him, it is also important to increase PR activities against the Egyptian regime.

Nigeria

The "Group of the People of Sunnah for Preaching and Jihad" (formerly known as Boko Haram) increased its PR activities in January-February, the results of which differed to some extent in their level of quality. Abubakar Shekau, the leader of the organization, threatened several times to attack Chad, Niger and Nigeria due to their decision to band together to establish a African regional force to work to eradicate the organization and restore security to the region. According to him, this coalition is doomed to fail and its members will pay a heavy price.

An important turning point for the organization took place with its oath of allegiance to the IS in the beginning of March 2015. This event also occupied the discourse on jihadist Web forums and among jihad fighters who welcomed this trend.

Jihadist Propaganda

- Al-Hussam Brigade, a media group that distributes online materials related to Al-Qaeda in the Arabian Peninsula (AQAP), called on its supporters several times during January-February 2015 to open a virtual workshop to serve as a platform for the distribution of jihadist materials on social networks as part of a PR campaign for the organization. On January 14, 2015, for example, the group noted that, in the framework of the online campaign, an AQAP video should be distributed on social networks regarding the claim of responsibility for the attack in Paris that took place in the beginning of January 2015. [2]

The logo of the media group, Al-Hussam Brigade

- Supporters of the IS established a special Web site named "5elafabook" (khilafah book as a reference for Facebook) designed to distribute the organization's PR material. The site's

[2] https://twitter.com/al_husam_nasher

configuration and its name are very reminiscent of the Facebook social network but its operations ceased the following day. An announcement published in English on the site stated that the reason for the site's temporary closure was due to the desire to protect the security of its members. It also stated, "We are back again because the site "5elafabook" is an independent site not affiliated with the Islamic State. The purpose of its establishment is to clarify to the world that we do not only carry weapons or live in caves as you tell yourselves. The Web site itself was launched in seven languages: Dutch, English, Spanish, Portuguese, Turkish and Indonesian". It would be interesting to know why the site ignored the French and Arabic languages.[3]

Defensive Tactics

- A visitor to the Shumukh al-Islam jihadist Web forum published a guidebook about computer security and protection. In addition to explanations, the guidebook included downloadable software designed to protect computers from viruses and spyware. For example, the visitor recommended using the Kaspersy Total Security and Zemana Antilogger software to protect against viruses and Trojan horses. According to the visitor, Tor the best browser to use when browsing the Web because it is encrypted and makes it difficult for intelligence agencies to discover the identity of the users. He also recommended using the comodo icdragon browser. In addition, the visitor recommended using an encrypted program for sending instant messages, such as Telegram, which can be installed on cellular devices and computers. [4]
- A writer affiliated with the IS, known as Abu Irhim al-Libi, published a two-part article for IS

[3] http://www.aljazeera.net/news/international/2015/3/10/أنصار-تنظيم-الدولة-يطلقون-موقعاً-على-الإنترنت

[4] https://shamikh1.info/vb/showthread.php?t=233259, https://dump.to/PcPr01

operatives on how to securely use the social network, Twitter. In the first part of the article, he explained that the US government invested 1.3 billion dollars in order to fight against the IS in the Twitter arena alone. According to him, the US government is continuously tracking the activities of IS operatives on social networks and is concentrating significant efforts on fighting the organization on this front. Therefore, he emphasized that IS operatives must take a series of steps in order to maintain their security while using social networks, specifically Twitter. In the framework of taking precautions, the writer recommended that IS operatives follow the Twitter account of Abdullah al-Ali, a Kuwaiti expert on IT security and CEO of Cyberkov Ltd. (https://twitter.com/3bdullla), for updated information that he provides about online security measures. In addition, the writer emphasized that one should not trust anybody on the Internet and should avoid providing identifying information to people even if they have prior familiarity with them because the online correspondence of IS operatives is being tracked. All those seeking to coordinate or to reach the arena of jihad via the Internet should avoid doing so. The Internet must serve only as a general guide and any coordination regarding a specific action must only take place with operatives in the field. Nevertheless, the writer suggested that all those who wish to help the IS should organize themselves in small groups, even if only composed of two people experienced in publishing jihadist materials, while being careful not to provide identifying information on social networks. In addition, he suggested creating several Twitter accounts simultaneously in case the Twitter management should close one of them.[5]

In the second part of the article, the writer provided a list of Twitter accounts that fight against the IS on Twitter. He emphasized that one should avoid entering these accounts, he published a list of these accounts, and he advised readers to block them through the site, blocktogether. He noted, for example, a hacker group from Japan that recently joined the battle on Twitter against the organization and recommended blocking the group’s Twitter account: https://twitter.com/opantiisis.[6]

[5] http://justpaste.it/twit

[6] https://justpaste.it/twit2

The banner of an article written for IS operatives on how to properly use Twitter

- During January-March 2015, a prominent activist calling himself "The Islamic State's Technology Expert", and who is affiliated with the Islamic State (IS) on social networks, published several guidebooks and precautions on various topics, including:
    - An article titled, "The Electronic War and the Disregard Shown by Supporters of the Islamic State". According to the writer, the activities of IS supporters on the social network, Twitter, are on a constant rise and include over 50,000 activists to date. However, the writer expressed distress over the level of awareness regarding exercising caution when using Twitter: "It is likely that out of every 100 supporters, only one of them pays attention to electronic security, as with the mujahideen". According to him, the British newspaper, *The Guardian*, published an article according to which a jihadist had tweeted a post on Twitter without realizing that the GPS on his cell phone was working at the same time. According to him, the US Army attributes equally considerable importance to electronic warfare as it does to nuclear warfare. Local and international intelligence agencies have the ability to track and identify the location of Web users, they know what they are watching on their computer and mobile phone, and they can even take photographs with the embedded camera on the computer and mobile phone. Therefore, it is the responsibility of IS supporters who have technological knowledge to share their professional knowledge and publish it everywhere in order to prevent their fellow supporters from falling prey to intelligence agencies. To date, 60 countries are waging an electronic battle against IS operatives while the awareness and self-defense shown by IS supporters on the Internet is catastrophic. In light of this, every IS supporter must take security measures and use computers and mobile phones in the

proper way.[7]

- A series of lessons concerning safety rules for using mobile phones. The first lesson deals with permissions for mobile phone applications. According to the writer, there are applications that request permission to access the device's camera and pictures, such as Skype. According to him, there is concern that the execution of this option could transmit sensitive material to intelligence agents and expose the identity of the users. In light of this, the writer proposes how to overcome this obstacle by installing software such as Dcentral and f-secure, which are designed to protect the privacy of the users.[8]

  In the second lesson, the writer discusses methods of encryption on iPhone and Android devices in order to protect them from hackers and intelligence agents. For example, he referred to a link - https://blog.cyberkov.com/2002.html – containing a detailed explanation on this topic.[9]

  The third lesson deals with fundamental security measures for the Android device. For example, the writer recommends installing the ORBOT application in order to encrypt the device, the FAKE GPS application in order to provide incorrect information about the user's physical location, and the D-VASIVE PRO application in order to protect the device against spyware.[10]

  In the fourth lesson, the writer recommends installing Cyanogenmod Rom, an operating system for Android that underwent modification by the developers. According to the writer, this version is preferred for its higher speed and its ability to encrypt the device.[11]

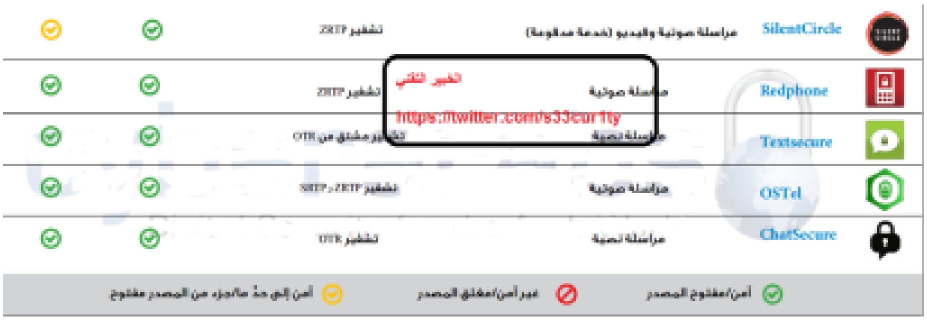
[7] http://justpaste.it/iq2p
[8] http://justpaste.it/iyas
[9] https://dump.to/ae9
[10] https://dump.to/ahc
[11] https://dump.to/Aa

In the fifth lesson, the writer recommends installing the keypad/keyboard application, a.i.type keyboard, in order to encrypt text while writing messages.[12]

In the sixth lesson, the writer discusses vital applications for Android and alternatives to the services offered by Google. For example, the writer suggests that readers stop using the Google store, which he claims includes a long list of fake applications that contain viruses and user tracking capabilities. In its place, he recommends that they use the Russian application store, yandex (http://m.store.yandex.com). Instead of using the Gmail email service, he suggests using the encrypted email software, tutanota. In place of google drive, the writer suggests using MEGA and copy sites. Other applications recommended by the writer included: pixlegarde – camera, and AD BLOCK PLUS – advertisement blocking.[13]

○ Recommendations for mobile phone applications and a list of applications that should not be used.[14]

[12] https://dump.to/arw
[13] https://dump.to/arO
[14] http://justpaste.it/iq6x



✓	✓	تشفير ZRTP	مراسلة صوتية وفيديو (خدمة مدفوعة)	SilentCircle	
✓	✓	تشفير ZRTP	مراسلة صوتية	Redphone	
✓	✓	تشفير مشتق من OTR	مراسلة نصية	Textsecure	
✓	✓	تشفير ZRTP، SRTP	مراسلة صوتية	OSTel	
✓	✓	تشفير OTR	مراسلة نصية	ChatSecure	

✓ آمن إلى حدّ ما/جزء من المصدر مفتوح　　🚫 غير آمن/مغلق المصدر　　✓ آمن/مفتوح المصدر

الخبير التقني

https://twitter.com/s33cur1ty

A chart posted by the writer containing secure applications for use on mobile phones

- A guidebook for protecting the Windows operating system, in the framework of which the writer recommends using the zemana anti-logger software in order to protect the computer from hacker breaches and information theft.[15]
- Correspondence titled, "Farewell to Google and Yahoo…and Welcome to Encrypted Email". According to the writer, the email services provided by Google, Yahoo and Hotmail have become a tool used by American intelligence agencies to gather information on users and spy on them. In light of this, the writer recommends leaving these companies and opening new email accounts on three alternative sites that offer encrypted email: proton mail, Toutanota and HUSHMAIL. Along with this advice, the writer provides a detailed and illustrated explanation of how to open an email account on these sites.[16]

- An explanation regarding how to expose links and folders designed to spy on users. For example, the visitor recommends using the Web site, https://www.virustotal.com, in order to check if a certain site is infected with viruses.[17]
- An explanation regarding the removal of suspected spyware applications from mobile

[15] https://dump.to/axX
[16] https://www.mnbr.info/vb/showthread.php?t=80794&styleid=18
[17] https://dump.to/arS

phone devices.[18]

- A guidebook on installing an operating system named TAILS, which earned the nickname "the operating system of Anonymous". The operating system is based on Linux, which enables Internet browsing without leaving a trail. The operating system includes tools for encryption and privacy, as well as an Internet browser, instant messaging software, email, and tools for picture and sound editing. It can be installed with a DVD, SD card or USB flash drive.

Download the ISO image

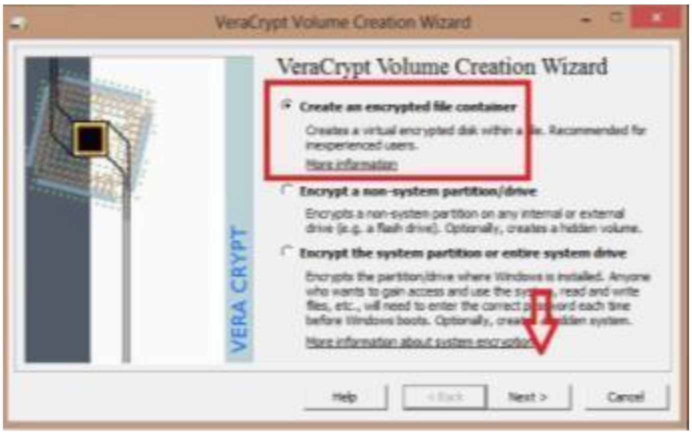
- An article titled, "The Electronic War and Disregard Shown by Supporters of the Islamic State". The article was based largely on the leaks by Edward Snowden, an American citizen who worked for the US National Security Agency (NSA) until 2013 when he defected to Russia after leaking sensitive information about the agency's cyber surveillance activities and drawing the attention of jihadists to the online spy operations being conducted by the American intelligence agency. For example, the writer of the article mentioned a software program called PRISM at the NSA that is designed to gather information about visitors to Web sites and companies that offer various online services to global audiences, such as Facebook, Yahoo, Google, Paltalk, YouTube, Skype, etc. This information includes photos, video clips, emails and other personal materials about users that are used by the intelligence agency to build profiles and a database. At the end of the article, the writer called on Web users who support the IS not to disregard their online safety by, among other things, using the TAILS operating system instead of

[18] https://dump.to/ary

Windows.[19]

- The fourth lesson in file encryption in the framework of a "course on computer safety [for] the Windows operating system". According to the author, the encryption of files and databases holds great importance that is ignored by the mujahideen and by those living in "heretical countries". According to him, it is not enough to use the TOR software to encrypt messages, but rather one must take into account that the personal material found on the back of the computer can be stolen if a hacker breaks into one's computer. In this context, he mentioned an article that was published in the magazine, *Foreign Policy*, on August 29, 2014, concerning important intelligence material that had reached foreign intelligence agencies. The material, which concerned biological weapons, was found thanks to the discovery of a computer belonging to an IS operative in Aleppo, Syria, after IS fighters had retreated from the area. According to the author, this sensitive information would not have reached foreign elements if that operative had been careful to encrypt his files and database: "Imagine, my brother, how beneficial this will be for the enemies of Allah". After clarifying this issue, the author recommended using an encryption software called "VeraCrypt".[20]

[19] https://dump.to/cyberwarfare
[20] https://dump.to/veracrypt



VeraCrypt Volume Creation Wizard

● Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

○ Encrypt a non-system partition/drive

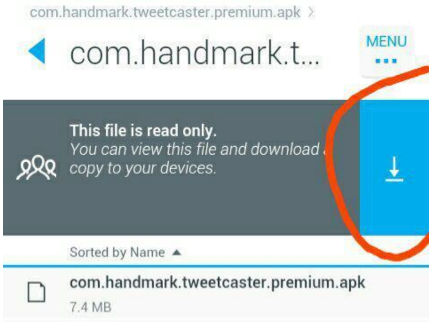
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

More information about system encryption

- ○ A recommendation for coping with the closing of IS accounts on Twitter. According to the writer, in order to make it more difficult for this to happen, it is best to use the application, TweetCaster, which tweets over 10 accounts at the same time.[21]



This file is read only.
You can view this file and download a copy to your devices.

com.handmark.tweetcaster.premium.apk
7.4 MB

- ○ The mapping of applications for Android worth downloading for safe surfing. Among the recommended applications: f-droid, YANDEX, DUCK DUCK GO, DROID WALL, and F-secure freedom. The mapping was published as lesson no. 8 in the framework of a course titled, “Securing Mobile Phone Devices”.[22]
- ○ A guidebook on USB encryption and removing folders using the “vera crypt” software. The guidebook was published as lesson no. 5 in the framework of a course titled, “A Course of Computer Security [on a computer installed with] the Windows Operating System”.

- Al-Raya jihadist media institution, which is affiliated with the Army of the Nation in Jerusalem – a Salafi-jihadist organization in the Gaza Strip, explained that caution should be used when

[21] https://dump.to/MercenariesTwitter
[22] https://dump.to/ANDROIDAPP

using Twitter. According to the media institution, in order to ensure proper use one must take a series of measures via the link, https://blog.cyberkov.com/1241.html. [23]

Offensive Tactics

- During January-February 2015, the "Army of Hackers" Arab Web forum for teaching hacking, published several guidebooks, including one on learning how to hack into Web sites using Android devices,[24] and a lesson on methods of hacking into Facebook accounts.[25]

Social Media

- The jihadist media institution of Al-Nusra Front in Syria, Al-Manarah Al-Bayda, posted a message to the media (no. 11); a clarification regarding the importance of adhering to the rules of publications concerning Al-Nusra Front on social networks. According to Al-Nusra Front, social networks play a significant role in many aspects of jihad, such as dawah and spreading the voice of the mujahideen from arenas of jihad. Nevertheless, it emphasized that there are those who exploit social networks to spread false messages in order to sow division among the ranks of the mujahideen. In light of this, Al-Nusra Front clarified that anyone caught breaking the publication rules and trying to sow the seeds of division and separation will be taken to task and immediately dismissed from Al-Nusra Front.[26]
- The Rabitat al-Ansar jihadist media institution, which is involved in PR for the Islamic State, tweeted on January 31, 2015 that France had launched a PR campaign aimed at slandering the name of the IS, under the hashtag #StopDjihadisme. According to the media institution, 60 million dollars were invested in the campaign, demonstrating how important it is to France. The media institution then asks IS supporters, especially those among them who speak French, to intervene in this discourse. Visitors identified with the organization expressed a willingness and agreement with the request, and offered to publish correspondence in praise of the organization in English or to publish photos for those who are not proficient in French. Another visitor noted that they can also publish in Arabic and those who want to understand the

[23] https://al-fidaa.com/vb/showthread.php?t=106723
[24] http://www.aljyyosh.com/vb/showthread.php?t=53980
[25] http://www.aljyyosh.com/vb/showthread.php?t=53952
[26] https://al-fidaa.com/vb/

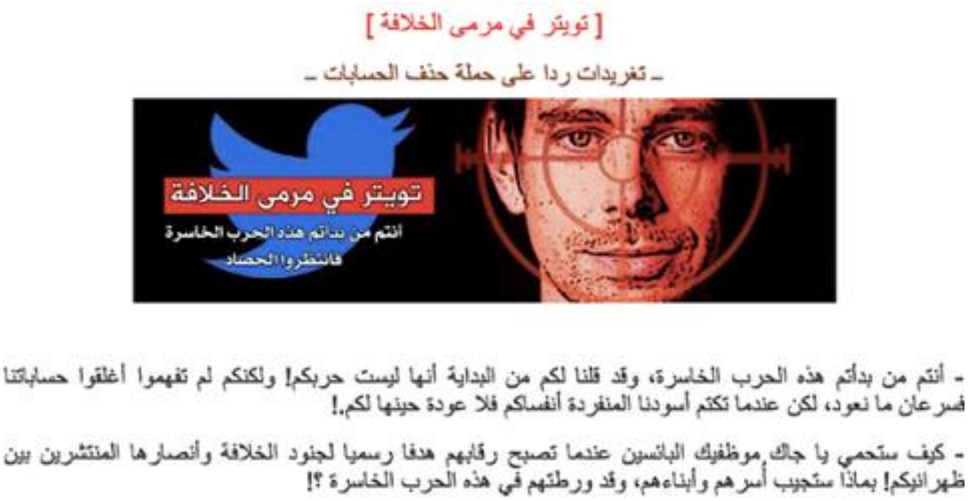
meaning of the text can use translation. The involvement of IS operatives and supporters under the above-mentioned hashtag was characterized by calls for more jihad in France and Europe.

- The Rabitat al-Ansar jihadist media institution advised one of its visitors (@hax3or) to contact an activist and supporter of the organization (@Abu_Seeraj) regarding the above-mentioned topic.[27]
- PR activists for the IS on social networks noted that the IS intends to launch a new television station to operate in Mosul, Iraq, and on the Internet called, "The Caliphate Channel", which will broadcast news concerning the organization. According to the activists, the channel intends to make live broadcasts as well. [28] In addition, the activists published a link to a promotional clip about the intention to launch this channel.[29]

A clip from the video

- On February 28, 2015 Al-Nusra al-Maqdisiyya, a Palestinian media group involved in PR for the IS, published a photo of Twitter founder, Jack Dorsey, on social networks and threatened him and his employees that they will be severely punished should they continue to remove and shut down Twitter accounts belonging to the IS. [30]

[27] https://twitter.com/anssaar112/status/561601495578075136
[28] https://twitter.com/s_abo_dojana/status/556072138860662785
[29] https://www.youtube.com/watch?v=5pK-lZTLvVU
[30] https://www.mnbr.info/vb/showthread.php?t=82659



[تويتر في مرمى الخلافة]

ـ تغريدات ردا على حملة حذف الحسابات ـ

- أنتم من بدأتم هذه الحرب الخاسرة، وقد قلنا لكم من البداية أنها ليست حربكم! ولكنكم لم تفهموا أغلقوا حساباتنا فسرعان ما نعود، لكن عندما تكتم أسودنا المنفردة أنفاسكم فلا عودة حينها لكم.!

- كيف ستحمي يا جاك موظفيك البائسين عندما تصبح رقابهم هدفا رسميا لجنود الخلافة وأنصارها المنتشرين بين ظهرانيكم! بماذا ستجيب أسرهم وأبناءهم، وقد ورطتهم في هذه الحرب الخاسرة ؟!

The posted threat against the Twitter founder and employees

The Charlie Hebdo Terrorist Attack in the Jihadist Discourse on Social Networks

The terrorist attack at the French magazine, *Charlie Hebdo*, which took place on January 8, 2015, triggered a frantic discourse on social networks by jihad activists and by official jihadist media institutions. Many jihad activists praised the attack, described it as a heroic action and called on Muslims to respond in the same manner to anyone who insults the Prophet anywhere in the West. Other jihad activists noted that the attack was a response to the participation of coalition forces against the IS in Iraq and Syria, and they called for a continuation of this line of attack as an expression of support for the IS. Others, including the radical preacher, Anjem Choudary, who lives in London, noted that freedom of expression has its limitations and that sometimes it exacts a high price when it ignores the rights of Muslims or hurts their feelings. Still others noted that the attack itself represents them, as noted by the title of the hashtag: “I am a Muslim, the attack on Charlie Hebdo represents me”.[31]

Other visitors expressed joy at the growing sense of fear among French civilians in light of the wave of terrorism gripping France. According to one of them, this constitutes a tremendous success and a disgraceful defeat for the French government due to the need to send in many army forces, tanks, planes and soldiers in order to deal with only two or three terrorists. In another discourse titled, “Lone Wolves Cast Fear in France”, jihadists called for this pattern to be emulated and for the wave

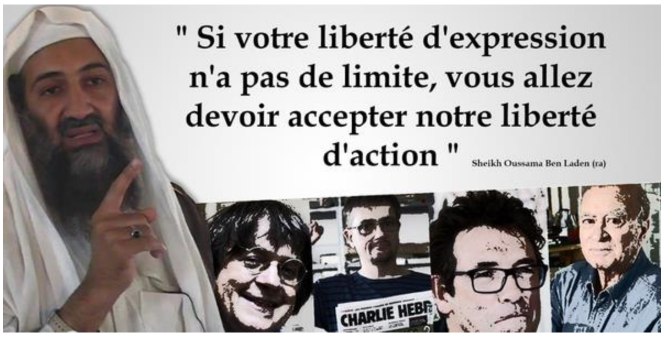
[31] #انا_مسلم_حادث_شارلي_ايبدو_يمثلني

of attacks against France to continue.[32]

Another visitor offered a conspiracy theory according to which the attack was designed by the Zionists in order to damage the image of Islam and the Arabs as a result of the decision made by several European governments to recognize the establishment of a Palestinian state.

The discourse on social networks among jihadists focused on several hashtags under various headings, such as: “Paris is Burning”,[33] “Muslims are Helping Their Prophet”[34] and “Our Revenge for the Sake of the Prophet”.[35]

A collection of photos on the topic:


" Si votre liberté d'expression n'a pas de limite, vous allez devoir accepter notre liberté d'action "
Sheikh Oussama Ben Laden (ra)
CHARLIE HEBD

“If your freedom of expression knows no limitations, then you will be deserve to suffer our freedom of action”[36]

A photo that was posted to Twitter under which it is written: “The attack on the newspaper that published insulting photos of the Prophet represents me”

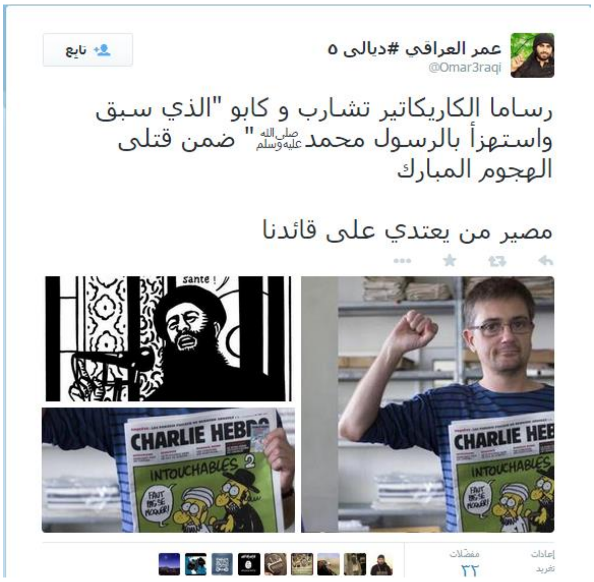
[32] #الذئاب_المنفردة_ترعب_فرنسا

[33] #باريس_تشتعل,

[34] #المسلمون_ينتصرون_لنبيهمﷺ

[35] #إنتقمنا_للرسول

[36] 7.1.14. https://twitter.com/SGHURABAA/status/552842952494813184



عمر العراقي #ديالى ٥
@Omar3raqi

رساما الكاريكاتير تشارب و كابو "الذي سبق
واستهزأ بالرسول محمد ﷺ" ضمن قتلى
الهجوم المبارك

مصير من يعتدي على قائدنا

A post by a jihadist praising the killing of the illustrator who insulted the Prophet Muhammad, “This is the fate [awaiting] those who attack our leader”

FRANCE – MALCHANCE
FINI : MÉTRO, BOULOT, DODO!!!
Oum chahid adam karim EL MEJJATI
الجبهة الإعلامية
للإعلام

“Paris is Burning” – a song clip that was posted by the Al-Ghuraba jihadi media institution, which is involved in PR for the Islamic State - to Twitter in praise of the attacks against France[37]

Organizational Activities

The Islamic State

Members of the IS are using a variety of Web sites and online social networks, with emphasis on spreading the organization’s messages, recruiting supporters and activists, and even sowing fear and terror using various clips of killings. However, the nature of this space - which provides instant communication from anywhere in the world to anywhere in the world and from any device, the relative anonymity, the great dependency on online information and the increasing dependency on computer systems, is turning it into an ideal tool for terrorists. It can also have a psychological

[37] http://justpaste.it/iswb

effect as well as cause economic and physical damage to the management of a modern state, without any need for the existence of a physical military force or its operation overseas. This activity enables a battle against remote enemies, irrespective of distance and borders, which hurts them in a way that is not possible since the Islamic State's physical presence is currently limited to the Middle East and North Africa. Therefore, if the organization continues to grow, develop and gain a stronger physical grip, and if it continues to win the hearts of supporters, we may find ourselves facing a new wing of this organization – the Cyber Islamic State – whether as an actual branch of the organization or as a conceptual branch by virtue of its activities being directed to the cyber realm.

The assumption is that this organization will turn more to cyber activities in order to create physical consequences; to garner online support for its physical battles, to wage psychological warfare and online fraud operations, and to create damage in the cyber realm that will result in physical damage.

For this reason, it is likely that an increase in cyber activity will include various aspects of these operations. In the area of online support for physical battle, we can see an increase in Internet use in several aspects:

- Online intelligence gathering - against individual and corporate targets in the Middle East and beyond.
- Winning hearts and minds – creating a large-scale online system in various languages in order to spread the organization's ideology via blogs, Web sites, forums and social networks; creating an array of religious clerics who swear allegiance to the organization and become its mouthpieces in the online arena via independent Web sites or as part of the organization's online activities; increasing the online recruitment of fans, supporters and even activists to the ranks of the organization.
- Online communication channels – the establishment of multimedia units in order to document the organization's terrorist activities and the training of local teams; the creation of an online array of channels for distributing news, videos and media activities, including documentation of terrorist attacks and information via social networks and Web sites. Due to the enormous dependence on information that comes from online content, and in light of past experience with **online psychological warfare**, we can see an increase in the use of the Internet for this

purpose through breaches of media Web sites and the planting of fake news items in order to create confusion as well as and public and economic anarchy among the organization's enemies. We can also see an increase in the use of the Internet for sowing fear among the organization's enemies, with emphasis on visual images.

Another use of online information as a tool of the organization can be seen in the **leaks** of massive amounts of information from a variety of targets considered to be enemies of the organization in the Middle East and around the world. The purpose of the leaks is to cause embarrassment to companies and countries, expose state interests and behind-the-scenes activities, and even conduct economic blackmail of countries and organizations.

Regarding **cyber activities intended to wreak damage**, the assumption is that it such activities will be carried out in several ways: attacks openly associated with the 'Cybernetic Islamic State' and/or by the creation of "cyber popular uprisings", and unidentified direct attacks based on the methods of operation used by 'Anonymous'. This is in order to create waves of cyber-attacks against companies, organizations and countries around the world, including those carried out in a coordinated fashion and those carried out as a popular initiative by supporters.

In this framework, emphasis will be placed on the following methods of operation: **Internet attacks** – attacks that deny service and damage sites, carried out by fans and supporters around the world. **Cyber-attacks** – attacks on physical infrastructure by hackers, including SCADA systems. **Hybrid attacks** – integrated and well-planned cybernetic physical attacks as well as **cybercrime** attacks, which can include online trading activity on the darknet as one of the organization's funding channels, online financial scams, and theft of money from banks and companies.

The assumption is that these activities will require the **establishment of a cyber-force**, local or foreign, with the following methods:

- The training of outstanding activists as expert hackers by friendly intelligence officials and as experts in the fields of cyber security.
- Amateur hackers around the world who operate independently as "lone wolves" for the sake of the general ideology, but not necessarily with direct intent.
- The creation of sleeper cells of hackers around the world.
- Existing groups of hackers that swear allegiance to the Islamic State.

- Hiring the services of professional hackers and cybercriminals
- Cooperation with the intelligence agencies of countries with interest and proven cyber capabilities that carry out attacks in the name of the organization.

In addition, there are attempts to implement aspects of **cyber security**, especially due to the extensive network of supporters and activists, a situation in which Internet and cellular communication has a valuable advantage but are also vulnerable. In this framework, they will be equipped with tools and technologies for executing various cyber-attacks and communication between activists, fans, supporters and even the organization's leadership, and will seek to develop an awareness of cautious online behavior for activists and supporters in order to prevent being tracked and located by foreign intelligence agencies.

This Internet and cyber activity is liable not only to deepen the Islamic State's operational, economic and ideological support base, but is also likely to cause psychological and even physical damage mainly in modern countries whose infrastructure relies on computer systems and the Internet.

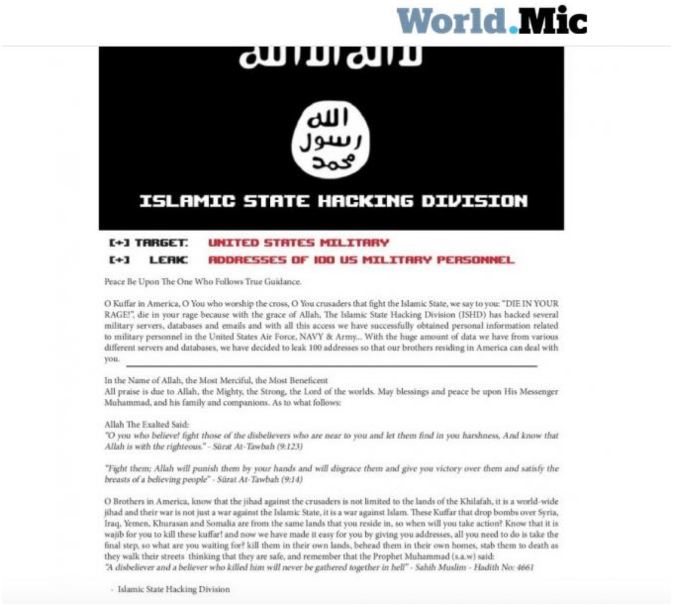
Several cyber-attacks took place during January-March, including breaches of Web sites, social network accounts and information leaks carried out by IS supporters. Some of the attacks were carried by groups or individuals that had previously acted against various targets such as Israel or the United States, but others were carried out by new groups and even those that claimed to be official units operating under the leadership of the organization:

On January 2, Islamic State Supporters hacked into the YouTube and twitter accounts of the US Central Command (CENTCOM) military forces in the Middle East and Asia. As part of the deferment, the twitter avatars were changed to IS images and tweets depicting actual infiltration into military bases were sent out. The breach made many experts worry that classified information had truly been compromised but now many believe the breach did not actually reach any private data. The breach is being referred to as "more embarrassing than destructive."[38] Additionally, a February 12 message from an IS supporters targeted a military wife who was written about in a CNN story regarding January's CENTCOM hack.[39]

[38] http://www.theguardian.com/us-news/2015/jan/12/us-central-command-twitter-account-hacked-isis-cyber-attack

[39] http://www.katu.com/news/local/ISIS-hack-attack-targets-local-military-wife-291601741.html

- On January 13, the Australian Communications and Media Authority issued warnings to Australia's citizens, encouraging people to be careful about links and emails they open in their email accounts. The emails reportedly contain the subject "ISIS attacks in Sydney?",[40] and play upon peoples' fears in the wake of the recent attack in Paris.
- On January 15, CENTCOM's Twitter account was hacked and a threatening tweet was posted: "AMERICAN SOLDIERS, WE ARE COMING, WATCH YOUR BACK". In addition, the attacker posted a list of army personnel that was most likely gathered from open source or leaked databases on the Internet. This act constituted psychological warfare as the CENTCOM messages said, "We won't stop! We know everything about you, your wives, and your children. U.S. soldiers! We're watching you!"[41]
- While the Islamic State Hacking Division had been publishing information about US military members throughout the month, some of the experts claim that the Islamic State's hacking skills are not as impression as they would like us to believe.[42]



ISLAMIC STATE HACKING DIVISION

[+] TARGET: UNITED STATES MILITARY
[+] LEAK ADDRESSES OF 100 US MILITARY PERSONNEL

Peace Be Upon The One Who Follows True Guidance.

O Kuffar in America, O You who worship the cross, O You crusaders that fight the Islamic State, we say to you: "DIE IN YOUR RAGE!", die in your rage because with the grace of Allah, The Islamic State Hacking Division (ISHD) has hacked several military servers, databases and emails and with all this access we have successfully obtained personal information related to military personnel in the United States Air Force, NAVY & Army... With the huge amount of data we have from various different servers and databases, we have decided to leak 100 addresses so that our brothers residing in America can deal with you.

In the Name of Allah, the Most Merciful, the Most Beneficent
All praise is due to Allah, the Mighty, the Strong, the Lord of the worlds. May blessings and peace be upon His Messenger Muhammad, and his family and companions. As to what follows:

Allah The Exalted Said:
"O you who believe! fight those of the disbelievers who are near to you and let them find in you harshness, And know that Allah is with the righteous." - Sūrat At-Tawbah (9:123)

"Fight them; Allah will punish them by your hands and will disgrace them and give you victory over them and satisfy the breasts of a believing people" - Sūrat At-Tawbah (9:14)

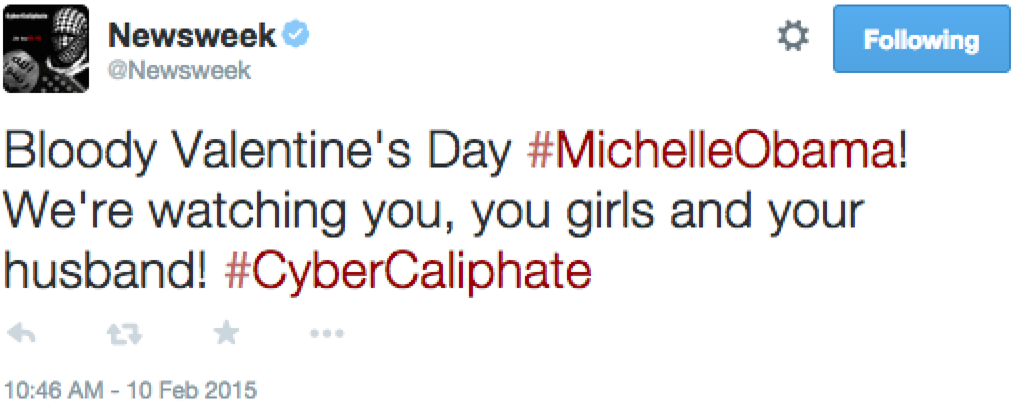
O Brothers in America, know that the jihad against the crusaders is not limited to the lands of the Khilafah, it is a world-wide jihad and their war is not just a war against the Islamic State, it is a war against Islam. These Kuffar that drop bombs over Syria, Iraq, Yemen, Khurasan and Somalia are from the same lands that you reside in, so when will you take action? Know that it is wajib for you to kill these kuffar! and now we have made it easy for you by giving you addresses, all you need to do is take the final step, so what are you waiting for? kill them in their own lands, behead them in their own homes, stab them to death as they walk their streets thinking that they are safe, and remember that the Prophet Muhammad (s.a.w) said:
"A disbeliever and a believer who killed him will never be gathered together in hell" - Sahih Muslim - Hadith No: 4661

- Islamic State Hacking Division

A screenshot of the Islamic State Hacking Division site publicizing military members' information

[40] http://www.dailymail.co.uk/news/article-2907703/Warning-threatening-fake-email-attachment-listing-locations-ISIS-plan-attack-year-used-infect-computer.html
[41] http://edition.cnn.com/2015/01/14/us/social-media-military-isis/
[42] http://mic.com/articles/113516/isis-claims-to-be-doxing-u-s-military-members-but-their-hacking-skills-need-some-work

- In late January and early February, the Web site of the Henry County Church in Henry County, Virginia was hacked by a group affiliated with the IS.[43] A Tennessee Westminster Presbyterian Church Web site was also hacked and a churchgoer claimed, "It's terrifying…you don't think about that type of thing happening in our area, I mean little town Johnson City, Tennessee."[44] Additionally, the Westminster Presbyterian Church in Martinsville, Virginia, was also the victim of a breach, similar to the Johnson City, Tennessee attack.[45]
- On February 10, the Twitter accounts of Newsweek Magazine and First Lady Michelle Obama were hacked. The main picture of Newsweek's Twitter account was changed to a masked man accompanied by the message, "Je sui IS IS", mocking the "Je Suis Charlie" and "Je Suis Juif" messages that flooded social media after the attacks in Paris and Tel Aviv. The group also used this platform to tweet offensive messages to Michelle Obama.[46] The hack is being investigated extensively.[47]



Newsweek
@Newsweek

Bloody Valentine's Day #MichelleObama! We're watching you, you girls and your husband! #CyberCaliphate

10:46 AM - 10 Feb 2015

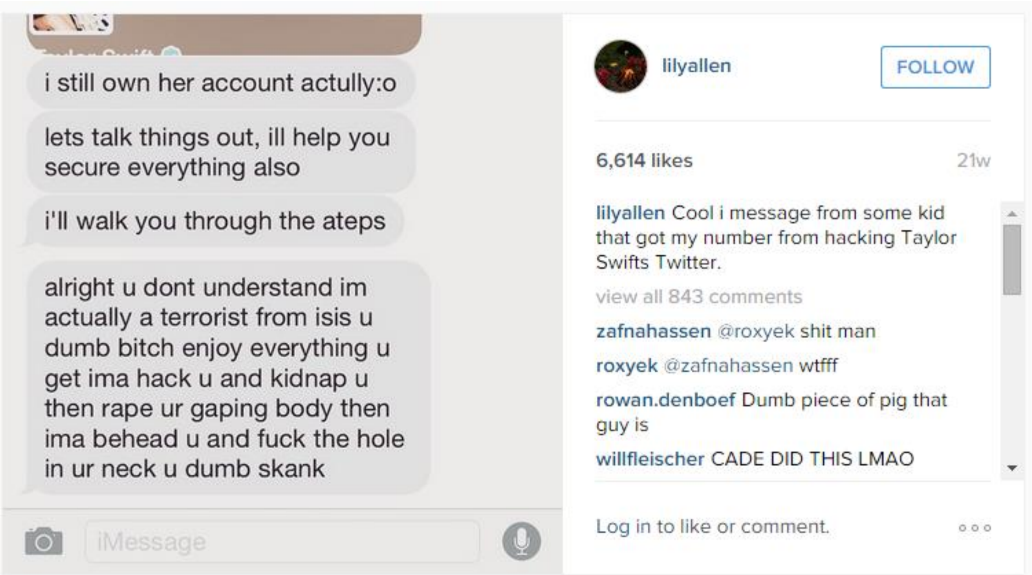
Screenshot of Newsweek's hack, displaying threatening messages to the First Family

- On February 11, Heybridge Swifts, of Essex, UK, was a victim of an IS affiliate cyber-attack.

[43] http://www.wdbj7.com/news/local/group-claiming-to-be-isis-hacks-website-of-henry-county-church/30970452
[44] http://www.christiantoday.com/article/us.churchs.website.is.hacked.by.isis/46774.htm
[45] http://www.worldmag.com/2015/02/hackers_loyal_to_isis_hit_pca_church_websites_others
[46] http://www.newsweek.com/newsweek-twitter-account-hacked-isis-affiliated-group-305897
[47] http://www.digitaltrends.com/mobile/newsweek-twitter-account-hack-obama-threat/

Officials believe the hackers confused the team to be a Premier League team.[48] This reaction is likely not the reaction that the hackers hoped to achieve.

- On February 13, the United Arab Emirate Web site was hacked by IS affiliates. As part of the defacement of the Web site, the hackers uploaded a picture of three militants dressed as soldiers in addition to logos regularly used by IS, including the Black Standard flag. The hacked Web site also displayed a photograph of Major Mariam al Mansouri,[49] the first female pilot in the United Arab Emirates. She is considered by the Islamic State to be an enemy because she has led strikes against the IS.[50]
- On February 14, British pop star Lily Allen received a threat from an IS supporter who hacked Taylor Swift's Twitter account. [51] The attacker used Swift's account to send a message to Allen:



i still own her account actully:o

lets talk things out, ill help you secure everything also

i'll walk you through the ateps

alright u dont understand im actually a terrorist from isis u dumb bitch enjoy everything u get ima hack u and kidnap u then rape ur gaping body then ima behead u and fuck the hole in ur neck u dumb skank

6,614 likes 21w

lilyallen Cool i message from some kid that got my number from hacking Taylor Swifts Twitter.

view all 843 comments

zafnahassen @roxyek shit man

roxyek @zafnahassen wtfff

rowan.denboef Dumb piece of pig that guy is

willfleischer CADE DID THIS LMAO

A picture posted on Allen's Instagram[52]

- On February 24, the Web site for the Chilean Ministry of Defense was hacked by the username "Sadam Husein." It displayed a message that, translated from Spanish, means:

[48] http://www.dailymail.co.uk/news/article-2949210/Islamic-State-s-latest-target-hacking-war-west-semi-professional-non-league-football-club-crowds-100.html
[49] http://www.newsweek.com/seditious-words-colorado-congressman-doug-lamborn-273985
[50] http://www.newsweek.com/website-uae-newspaper-al-ittihad-hacked-group-claiming-isis-affiliation-306808
[51] http://www.ibtimes.co.uk/lily-allen-posts-photo-abusive-messages-sent-by-isis-terrorist-1487963
[52] https://instagram.com/p/zBy2okwMVp/

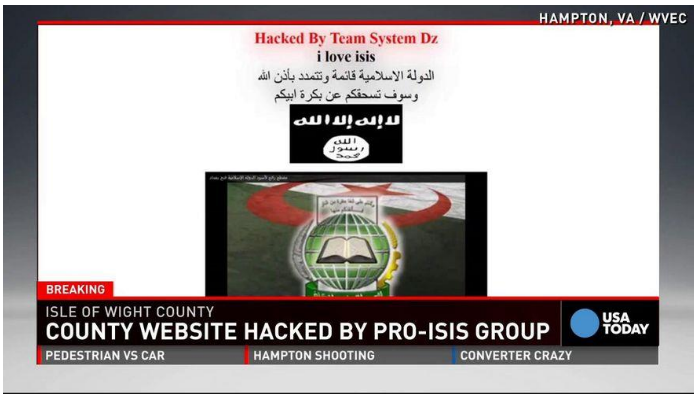
"We are ISIS, don't forget me." Classified information was not affected.[53]

DARKSHADOW HACKING GROUP

- On January 2, "Darkshadow," an IS affiliated hacking group also known as the "Arab Security Team", took over a Bristol, UK, bus system Web site. Officials believe the hackers thought the site was internationally affiliated, as opposed to being a small trip web site.[54]

TEAM DZ

- In the week of January 15, various Tennessee non-profit Web sites, New York newspaper sites, and Virginia government sites were hacked. The Web site for the government of the Isle of Wight County in Virginia was also hacked. Hosted by a third-party service, this was the second time in two weeks that the site had been hacked.[55]



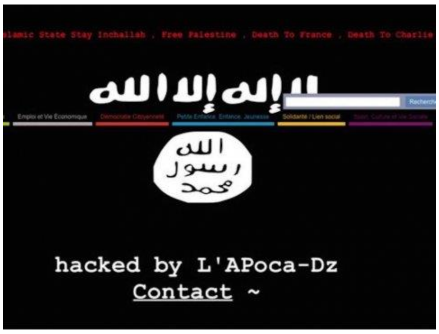
Hacked By Team System Dz
i love isis
الدولة الاسلامية قائمة وتتمدد بأذن الله
وسوف تسحقكم عن بكرة ابيكم

Screenshot of the Virginia website hacked by Islamic State supporters

- A hacking group affiliated with the IS hacked into a variety of Web sites. For example, in early January, the Buena Park non-profit site, "Giving Children Hope", was defaced and showed the message, "I love ISIS." Instead of being viewed as a completely random hack, "representatives for the Buena Park nonprofit said…it has been giving supplies to Syrian

[53] http://thestack.com/chile-ministry-defence-hacked-group-isis-240215
[54] http://www.inquisitr.com/1721870/isis-hackers-known-as-darkshadow-mistakenly-hack-bristol-bus-service-website/
[55] http://www.wfmynews2.com/story/news/2015/01/19/pro-isis-group-hacks-a-virginia-countys-website/21991927/

refugees in Lebanon, Turkey and Jordan since 2012."[56] In mid-January, just days after the *Charlie Hebdo* shooting, Team DZ also targeted and defaced Web sites displaying messages such as, "Death to France, The Islamic Stat Stay Inchallah, Free Palestine…Death to Charlie."[57] The site also displayed the messages, "Power of Algeria" and "Algerian to the Core."[58]



lamic State Stay Inchallah , Free Palestine , Death To France , Death To Charlie

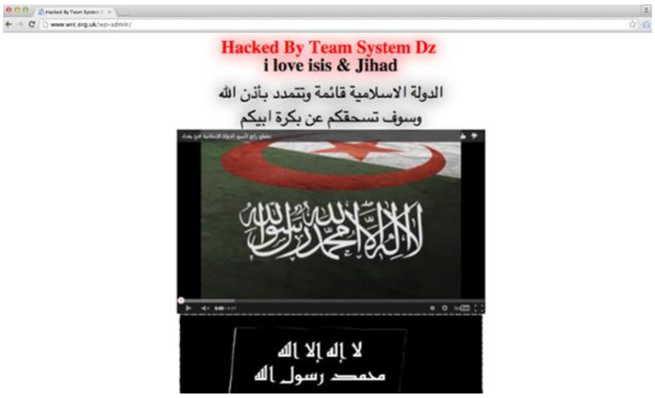
hacked by L'APoca-Dz

Contact ~

Screenshot of a hacked French Web site

- On January 20, the Web site for Chemeketa Community College in Salem, Oregon, was hacked by Team DZ and displayed the message "I love ISIS" as well as messages against Israel and France.[59] On January 21, Team DZ hacked 70 Web sites related to 40 Spanish cities. Some believe the attack was connected to a previous attack in France in which 20,000 French Web sites were shut down after being hacked by IS affiliates, while the *Charlie Hebdo* solidarity rally was taking place.[60] The site also displayed the message "Je suis Muhammad."[61]
- Algerian IS affiliates and Team DZ also hacked the Web site of a London women's group. The hack left members of the organization unsure of what the next steps would be.[62]

[56] http://www.ocregister.com/articles/children-647453-hope-isis.html
[57] http://www.businessinsider.com/isis-hack-french-websites-after-charlie-hebdo-shooting-2015-1
[58] http://rt.com/news/221131-hack-isis-france-charlie/
[59] http://www.statesmanjournal.com/story/news/2015/01/20/hack-redirects-chemeketa-website-visitors-pro-isis-page/22072963/
[60] http://rt.com/news/224755-isis-hacks-spanish-websites/
[61] http://www.thelocal.es/20150121/isis-hack-spains-town-hall-websites
[62] http://www.theguardian.com/voluntary-sector-network/2015/jan/29/london-charity-hacked-pro-isis-group



Hacked By Team System Dz
i love isis & Jihad

الدولة الاسلامية قائمة وتتمدد بأذن الله
وسوف تسحقكم عن بكرة ابيكم

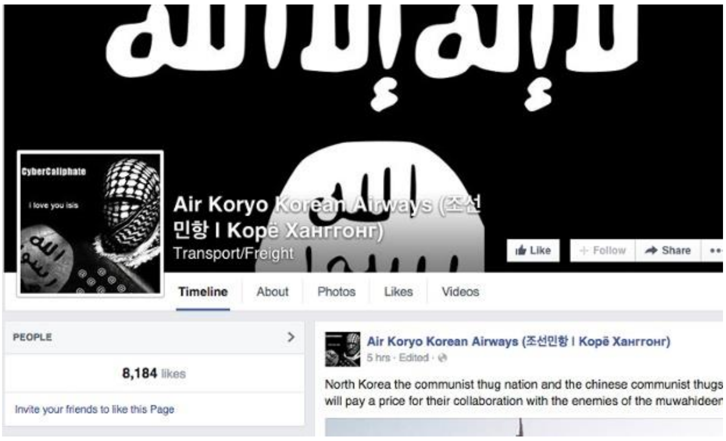
Screenshot of the hacked women's group site

CYBER CALIPHATE

- On January 12, CENTCOM social media accounts in Florida were hacked by CyberCaliphate and displayed threatening messages to American troops, including personal information about high ranking US generals.[63] This hack appears to be related to the January 2 CENTCOM hacks. On January 13, an extensive news report came out covering the CENTCOM hacks and experts claimed that the hack was likely carried out by the CyberCaliphate[64] but was likely not as threatening as initially assumed since the social media accounts did not allow the hackers access to any classified information, but rather simply allowed the hackers to display their messages.[65]
- Continuing their string of breaches, the CyberCaliphate hacked Maryland and New Mexico business Web sites, claiming "INFIDELS, NEW YEAR WILL MAKE YOU SUFFER."[66] CyberCaliphate also hacked New Mexico, Maryland, and Tennessee news Web sites.[67]
- The following week, on January 14, the Facebook page of the North Korean airline, Air Koryo, was hacked by Cyber Caliphate and the subsequent messages displayed called Kim

[63] http://www.dailymail.co.uk/news/article-2907040/ISIS-hacks-Central-Command-Twitter.html
[64] http://www.thedailybeast.com/articles/2015/01/12/isis-hackers-love-american-folk-punk-don-t-know-the-name-of-their-own-terror-group.html
[65] http://www.wired.com/2015/01/doesnt-really-matter-isis-sympathizers-hacked-central-commands-twitter/
[66] http://rt.com/usa/220595-fbi-isis-hacks-media/
[67] http://www.scmagazine.com/pro-isis-group-hijacks-twitter-accounts-of-local-media-outlets/article/391900/

Jong-un a “crying pig.”[68]



Air Koryo Korean Airways (조선민항 I Kopё Xahrohr)

Transport/Freight

8,184 likes

Air Koryo Korean Airways (조선민항 I Kopё Xahrohr)

5 hrs · Edited ·

North Korea the communist thug nation and the chinese communist thugs will pay a price for their collaboration with the enemies of the muwahideer

Screenshot of Air Koryo’s Facebook page during the hack of the social media site

- Demonstrating its influence on various social media platforms early in the week of March 11, the twitter hashtag #CyberCaliphate was widely trending as news of IS breaches made its rounds.[69] Law enforcement officials found that various American and Canadian businesses’ Web sites were defaced and the pages loaded with flash audio plugins of their music and propaganda.

  Their message was “we are everywhere.” All of the Web sites used WordPress platform. WordPress is an open-source platform and, therefore, it is easy to make changes to the sites, even for “script kiddies” (i.e. basic hackers).[70] The FBI is investigating the breaches in an attempt to cut down on their frequency, secure holes, and attempt to figure out where the infiltration is coming from.[71]
- A number of Ohio Web sites were hacked, but the breaches only affected the sites themselves and personal credit card information was not taken.[72]
- According to a report released on March 24 through Radio Fee Europe Radio Liberty, the

[68] http://www.theguardian.com/world/2015/jan/14/isis-hackers-north-korean-airline-facebook
[69] https://twitter.com/hashtag/CyberCaliphate?src=hash
[70] http://www.nbcnews.com/news/us-news/isis-hackers-almost-certainly-not-isis-hackers-n320296
[71] http://www.nbcnews.com/news/us-news/isis-hackers-almost-certainly-not-isis-hackers-n320296
[72] http://www.dispatch.com/content/stories/local/2015/03/10/hackers-strike-websites.html, http://edition.cnn.com/2015/02/10/us/isis-cybercaliphate-attacks-cyber-battles/index.html

Islamic State's "cybercaliphate" attacked over 600 Russian Web sites in 2014 alone[73]. The hacked sites vary in type, from banks to schools. In addition to the "cybercaliphate", other groups related to the attack included DZ and the Global Islamic Caliphate. A Russian researcher claimed that the IS will launch a cyber-attack on any country in order to instill fear and to appear relevant.

ISLAMIC STATE HACKING DIVISION

- On March 21, a group connected to the IS known as the ISHackingDiv published a list of home addresses and personal information allegedly belonging to members of the US military. The accompanying message claimed that sleeper cells in the United States would carry out attacks, specifically beheadings, and should do so in the soldiers' home country to show them that they are not safe anywhere. As of yet, the Department of Defense has not verified if the threat is credible. The list was published under the name "Islamic State Hacking Division."[74]

  The Twitter account of the new group was recently suspended.[75] Experts believe the breach was about "intimidation and propaganda"[76] more than actual threats. The IS claimed that the information was taken from "secure computers", while others argue that the information could be found online.[77]

ISIS CYBER ARMY

- On March 24, the ISIS Cyber Army released the following statement:[78]

Praise be to Allah, and peace and blessings be upon the Prophet Muhammad Sadiq promise Secretary.

[73] http://www.rferl.org/content/islamic-state-cybercaliphate-hacking-russian-websites/26920130.html
[74] http://www.washingtontimes.com/news/2015/mar/21/islamic-state-posts-kill-list-with-purported-address
[75] http://www.dailymail.co.uk/news/article-3005939/ISIS-publishes-kill-list-military-members-online.html#ixzz3V4vTifGx
[76] http://www.nbcnews.com/storyline/isis-terror/names-u-s-service-members-posted-online-group-claiming-be-n328186
[77] http://news.nationalpost.com/2015/03/22/isis-linked-group-releases-hit-list-of-u-s-military-personnel-including-names-and-addresses/
[78] https://justpaste.it/isis-cyberarmy2

Oh God, we are not aware only Thou, art the All-Wise, God taught us what benefit us and Anfna including taught us and we have increased the note, and show us the right to really grant us his followers, and show us the falsehood and grant us to avoid, and make us listen to those who say tracking Well, we have introduced mercy in slaves righteous

The praise of God proceeds to penetrate 29 site and thankfully…

…Each of (America # # # Nigeria Netherlands # # France Russia)

To support the # Ath_alasalamah

Date with penetration

American sites with registration and images site

Your brother in God

Hacker Caliphate State

isis_cyberarmy

- Addressing Allah, the hackers claimed that they plan to infiltrate, or have already infiltrated, a number of Western Web sites.[79] It is unclear what law enforcement plans to do, but it is likely that the Web sites will be examined and anti-hacking software will be implemented in order to minimize any damage the breaches may cause to the sites and systems, or any psychological stress that they could inflict upon the communities associated with any of the websites.

Cyber-attacks against the Islamic State

Cyber-attacks against the IS already began in June 2014 but due to the fact that IS was not an actual state with computer and communication systems, a computerized army or critical infrastructure, but rather only had some Internet activity, it could not be fought against online in the usual manner through breaches and leaks by government sites or attempts to shut them down, as 'Anonymous' did in its attacks against various countries and organization over the years, including Israel.

In this framework, the operations carried out by 'Anonymous' can be identified on two axes:

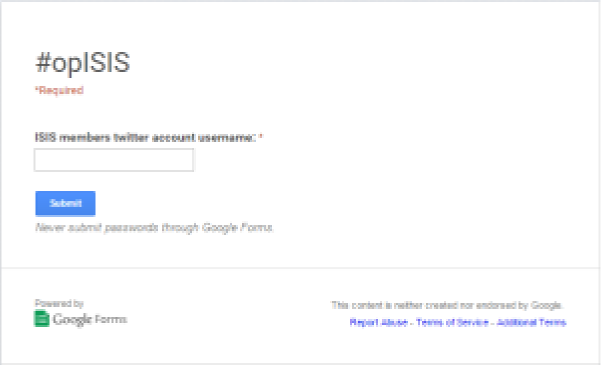
- **Attacks against the countries considered to be IS supporters and those that help the organization** – In June 2014, a video was distributed in the framework of OpNo2ISIS in

[79] https://justpaste.it/isis-cyberarmy2

which Turkey, Qatar and Saudi Arabia were named as the targets of the attack,[80] and threats were made to attack government sites in these countries. In September 2014, an interview with an alleged 'Anonymous' activist was published on the France 24 television station that contained another warning to these countries that if they continue to support the IS, those activists would be forced "to destroy their virtual infrastructure."[81]

- **Attacks against online activity attributed to the IS** – This includes attempts to disable the Islamic State's online activity since it is the organization's sole media channel and almost the only non-physical way to hamper the organization's activities. Such an attempt was made in the recent operation, OpISIS, in the framework of which many lists of Twitter accounts belonging to the IS were published for the purpose of monitoring them and shutting them down. One of the lists claimed to contain 1,012 Twitter accounts,[82] and another claimed to have over 900 accounts.[83] @AwayKuffr[84] surpassed them by publishing of a list of 2,484 Twitter accounts to be blocked,[85] and referred to a page with the option to block the accounts.[86] On February 23, it reported a page[87] based on Google Forms through which users could report Twitter accounts identified with the IS, [88] by using crowdsourcing to locate accounts of IS supporters.

[80] https://www.youtube.com/watch?v=_kJtvFUMELM
[81] https://www.youtube.com/watch?v=Cy9blSPn8nw
[82] https://ghostbin.com/paste/nfvej
[83] http://pastebin.com/nUC8PT4g
[84] https://twitter.com/AwayKuffr
[85] http://pastebin.com/6Q46bM0j
[86] https://blocktogether.org/show-blocks/c28a48c689efa78ce6dd308c4809406a3004b12d4ba4a3a5986e41cdc947f6a10daf93c96548f770f7285d38486ba60b
[87] https://twitter.com/4ngry_m4n/status/569879099046436864
[88] https://docs.google.com/forms/d/1DioA2X4wZ7wJN8_1-svJdwgmSXT1Y9qMz47oOJeatag/viewform?c=0&w=1



#opISIS

*Required

ISIS members twitter account username: *

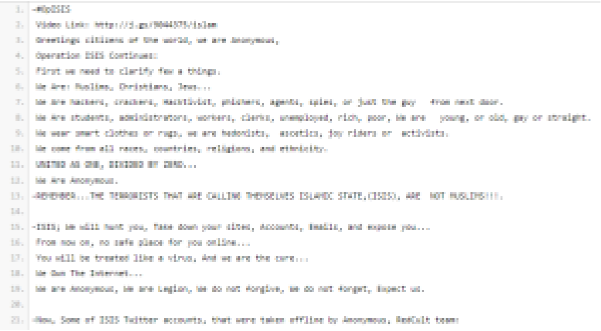
Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google.

A screenshot of a form to report IS members' Twitter accounts

in mid-March, a list in which is claimed to contain 9,200 Twitter accounts belonging to the IS was published online in order for user to block the accounts.[89]

Another list[90] includes a direct reference to IS members, claiming that they are not Muslims and that members of 'Anonymous' will chase them down, bring down their accounts and expose their identities, as did another list that was published in German.[91]



```
-#OpISIS
 Video Link: http://j.gs/9044375/islam
 Greetings citizens of the world, we are Anonymous,
 Operation ISIS Continues:
 First we need to clarify few a things.
 We Are: Muslims, Christians, Jews...
 We are hackers, crackers, Hacktivist, phishers, agents, spies, or just the guy   from next door.
 We are students, administrators, workers, clerks, unemployed, rich, poor, We are   young, or old, gay or straight.
 We wear smart clothes or rags, we are hedonists,  ascetics, joy riders or  activists.
 We come from all races, countries, religions, and ethnicity.
 UNITED AS ONE, DIVIDED BY ZERO...
 We Are Anonymous.
-REMEMBER...THE TERRORISTS THAT ARE CALLING THEMSELVES ISLAMIC STATE,(ISIS), ARE  NOT MUSLIMS!!!.

-ISIS; We will hunt you, Take down your sites, Accounts, Emails, and expose you...
 From now on, no safe place for you online...
 You will be treated like a virus, And we are the cure...
 We Own The Internet...
 We are Anonymous, We are Legion, We do not forgive, We do not forget, Expect us.

-Now, Some of ISIS Twitter accounts, that were taken offline by Anonymous, RedCult team:
```

Activists from 'Anonymous' also took action to bring down Web sites affiliated with the IS.[92]

This activity illustrates not only the power of the Internet and social networks to spread all types of information, but its value as the ideal tool for spreading the messages of organizations that lack any technological capability. This situation enables an organization like the IS to circulate text messages,

[89] http://xrsone.com/isis.htm
[90] http://pastebin.com/DhT8f2KZ
[91] http://pastebin.com/nuCYVgty
[92] https://twitter.com/DigitaShadow/status/569040785057951744

photos and videos in order to recruit supporters, activists and funds, and in order to sow terror and fear among its various enemies, without any need for a technological infrastructure and with almost no way to prevent its production and distribution of content around the world. Indeed, this is the mixed blessing and curse of modern technology in general, and of the Internet in particular.

The 'Syrian Electronic Army'

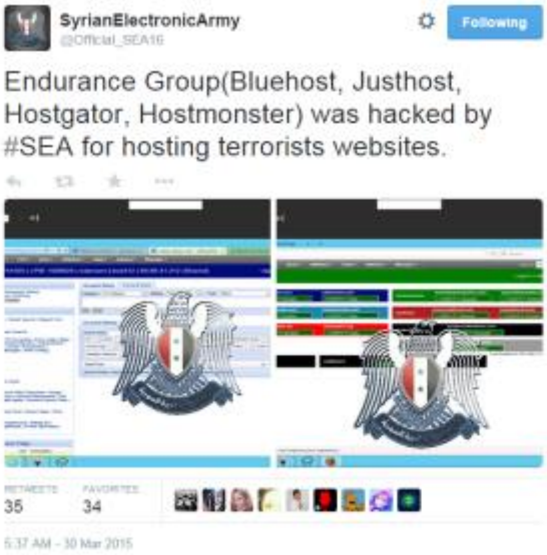
- On January 21, 2015 the 'Syrian Electronic Army' published an announcement according to which it had hacked into the Twitter account of the French newspaper, Le Monde.[93]
- On February 7, 2015 an announcement was published on the Twitter account of the 'Syrian Electronic Army' regarding the leak of Turkish government and army documents. The announcement[94] directs visitors to a page on the organization's Web site called Turkey Files, which was created on October 13, 2012.[95] This page includes 14 files containing documents, the most recent of which are from 2012. These files include the Prime Minister's Office, the Ministries of Defense, Foreign Affairs, Security, Industry, Presidency, the National Assembly and the Air Force, as well as files for several individuals.
- On February 11, 2015, the Web site of the Turkish *Hurriyet Daily News* published[96] an interview that was conducted with the spokesman for the 'Syrian Electronic Army' via email, following a report several days earlier, which stated that the group had leaked Turkish and Saudi army and government documents. These events indicate that activists managed to hack into hundreds of email accounts, including those belonging to the Turkish government two years earlier - according to the claim, in light of the downing of a Syrian helicopter by Turkish fire in September 2013. However, they waited for a politically ripe moment to expose the coordination between the Turkish government and armed groups in Syria in order to publish their findings, which included 967 email accounts in 14 categories and exposed correspondence between March 2009 and November 2012.

  According to the report, the SEA spokesman who answered Hurriyet's questions said: "The

[93] https://twitter.com/Official_SEA16/status/557713011117654017
[94] https://twitter.com/Official_SEA16/status/564139485676335106
[95] http://leaks.sea.sy/en/Turkey-Files
[96] http://www.hurriyetdailynews.com/syrian-hacker-group-says-it-hacked-turkey-two-years-ago.aspx?pageID=238&nID=78174&NewsCatID=352

whole world disrespected Syria’s borders; in return we too will disregard all the borders of the world and will target those who want to harm our country, no matter where they may be. We act independently and have a very large support base of members on social media… We are currently hosted on foreign servers. No one has lent their support to us but it is OK, because it doesn’t take much just a laptop, an Internet connection, knowledge and time."

- On March 30, 2015, the ‘Syrian Electronic Army’ announced that it had hacked into the Web sites of Web hosting companies belonging to the group, Endurance, which it claimed “hosts terrorist Web sites”.



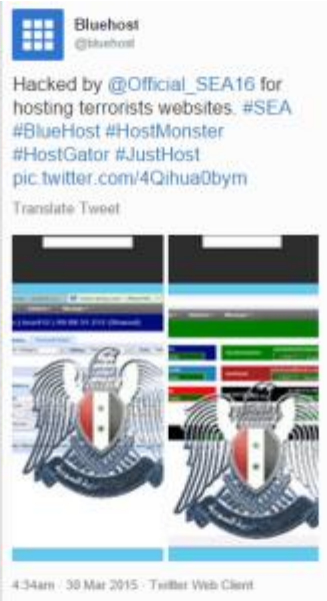
SyrianElectronicArmy
@Official_SEA16

Endurance Group(Bluehost, Justhost, Hostgator, Hostmonster) was hacked by #SEA for hosting terrorists websites.

RETWEETS 35
FAVORITES 34

5:37 AM - 30 Mar 2015

According to the announcement, the sites of four companies were hacked: FastDomain, HostMonster, HostGator and BlueHost, as well as the latter’s Twitter account, and two messages were posted to the account within a half hour and were deleted a short time after.



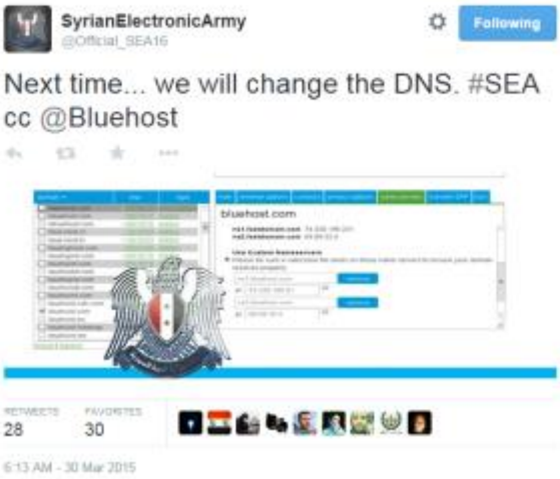
Bluehost
@bluehost

Hacked by @Official_SEA16 for hosting terrorists websites. #SEA #BlueHost #HostMonster #HostGator #JustHost pic.twitter.com/4Qihua0bym

Translate Tweet

4:34am · 30 Mar 2015 · Twitter Web Client

The group later posted another message in which it threatened future action against the company.[97]



SyrianElectronicArmy
@Official_SEA16

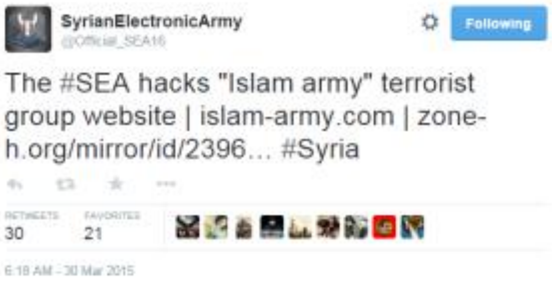
Next time... we will change the DNS. #SEA cc @Bluehost

RETWEETS 28
FAVORITES 30

6:13 AM - 30 Mar 2015

Meanwhile, the group announced that it had breached a Web site called islam-army.com, which is hosted on the BlueHost server, a move that apparently led to the breach of these companies' servers.[98]

[97] https://twitter.com/Official_SEA16/status/582380059375181825
[98] https://who.is/whois/islam-army.com



SyrianElectronicArmy
@Official_SEA16

The #SEA hacks "Islam army" terrorist group website | islam-army.com | zone-h.org/mirror/id/2396… #Syria

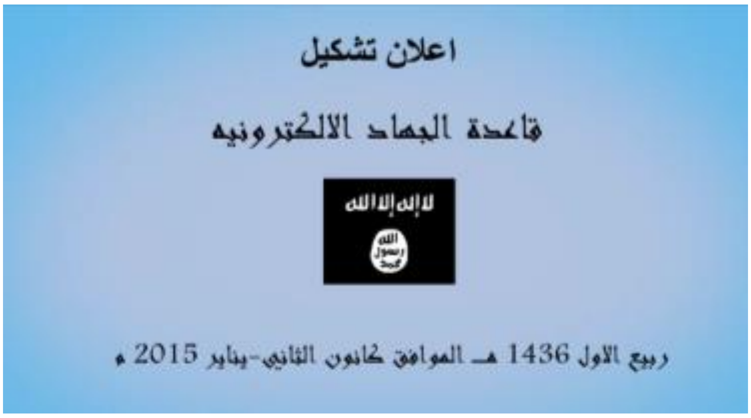
RETWEETS 30 FAVORITES 21

6:18 AM - 30 Mar 2015

‘Electronic Al-Qaeda’

- On January 20, 2015 an audio clip was published on the *Areen al- Mujahideen* jihadist Web forum in which it declared the establishment of a new hacker group called “Qaedat al-Jihad al-Elektroniyya” to serve as Al-Qaeda’s new wing in the field of electronic warfare. The spokesman on the audio clip praised Sheikh Ayman al-Zawahiri, the leader of Al-Qaeda, and noted that the group would help defend Islam from its enemies.[99]

  It should be noted that this announcement was not published via Al-Qaeda’s jihadist media institution, Al-Sahab, and therefore it should be treated cautiously. It is possible that the group does, indeed, identify with the concept of global jihad from the madrasa of Ayman al-Zawahiri but did not receive such approval from Al-Qaeda’s top leadership.



اعلان تشكيل

قاعدة الجهاد الالكترونيه

لا إله إلا الله
الله رسول محمد

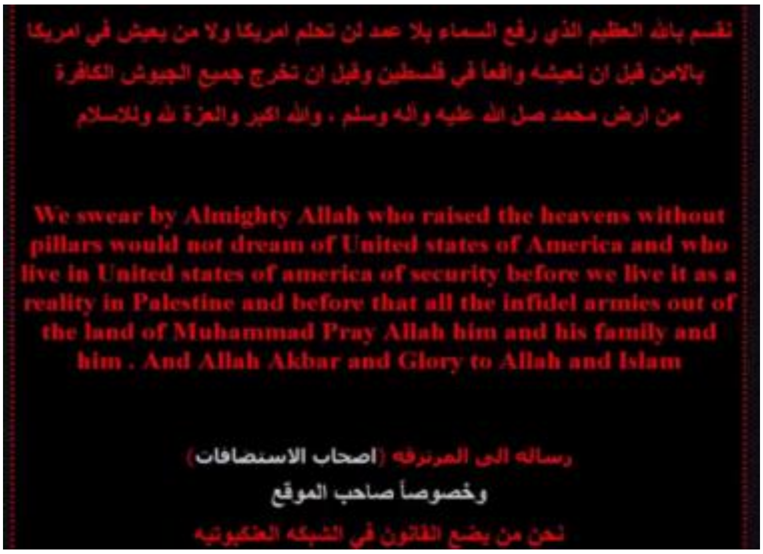
ربيع الاول 1436 هـ الموافق كانون الثاني-يناير 2015 م

The banner of the announcement regarding the establishment of a new hacker group

In January 2015, “Qaedat al-Jihad al-Elektroniyya” claimed responsibility for defacing the

[99] .20.1.15 http://www.al-aren.com/vb/showthread.php?t=7526

Web site of an American commercial company[100] and the Web site of a Christian church that, according to the group, had ridiculed and disrespected the Prophet Muhammad. [101] According to the group, the breaches and defacement were intended to strike at the economies of the US and its allies. In March 2015, the group claimed responsibility for the breach and defacement of four Israeli Web sites, [102] seven Chinese sites [103] and three Indian sites belonging to a large Indian commercial company that operates in the Indian subcontinent. [104] In April 2015, the group claimed responsibility for the defacement of a Web site belonging to a lawyers association in Vietnam. [105]



نقسم بالله العظيم الذي رفع السماء بلا عمد لن تحلم امريكا ولا من يعيش في امريكا
بالامن قبل ان نعيشه واقعا في فلسطين وقبل ان تخرج جميع الجيوش الكافرة
من ارض محمد صل الله عليه واله وسلم . والله اكبر والعزة لله وللاسلام

We swear by Almighty Allah who raised the heavens without pillars would not dream of United states of America and who live in United states of america of security before we live it as a reality in Palestine and before that all the infidel armies out of the land of Muhammad Pray Allah him and his family and him . And Allah Akbar and Glory to Allah and Islam

رساله الى المرتزقه (اصحاب الاستضافات)
وخصوصاً صاحب الموقع
نحن من يضع القانون في الشبكه العنكبوتيه

The message posted by the hacker group on an American commercial site

[100] https://www.youtube.com/watch?v=Sll50TQFGBA
[101] https://www.youtube.com/watch?v=RvgVHCESCx8
[102] https://justpaste.it/qe_b3
[103] https://twitter.com/GlobalJahadNetw/status/578351044155060224
[104] http://www.sunnti.com/vb/showthread.php?t=25927
[105] http://www.sunnti.com/vb/showthread.php?t=26192 . http://www.shabakataljahad.net/vb/showthread.php?p=111276

Screenshot of the site that was breached

RedHack

On January 16, 2015 the Turkish hacker group, RedHack, which operates regularly against Turkish government bodies, leaked over 4,000 telephone numbers belonging to employees of Turkcell, a Turkish cellular company.[106] In addition, the group carried out a DDoS attack against the Web site of the Turkish Central Bank to protest the devaluation of the Turkish Lira.[107] On February 3, the group announced that it had attacked two government sites – defacing one of them and leaking user names and access passwords from the other. The first announcement concerned the leak of user names and passwords from the Web site of metal industry workers union in Turkey, and referenced a file containing the access details.[108]

[106] https://www.hackread.com/redhack-leaks-4k-turkcell-numbers-against-facilitating-ministers-with-new-numbers/
[107] http://news.softpedia.com/news/Website-of-Turkey-s-Central-Bank-Disrupted-by-RedHack-417821.shtml
[108] https://twitter.com/RedHack_EN/status/562663135711338496

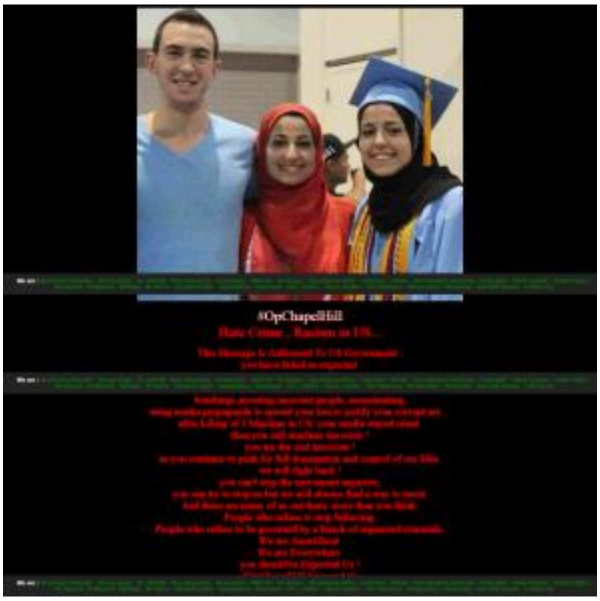
A short while later, another announcement was published[109] regarding the defacement of a Web site belonging to the Turkish Ministry of Economy. This hacker group mostly acts against Turkish government entities, including the defacement of a site belonging to the Istanbul Police Association,[110] the leak of information regarding the Mayor of Ankara,[111] and, most prominently, the breach of the payment site of Istanbul Province in which it published access information and erased citizens' debts.[112] On March 12, 2015 the defacement of the Istanbul Police Association was reported. The operation was carried out in memory of Berkin Elvan, a teenager who was killed during a demonstration in the beginning of 2014.[113]

AnonGhost

On January 1, 2015 the hacker group, AnonGhost, some of whose members express support for the IS,[114] published an announcement according to which it had obtained the WhatsApp account information of thousands of Israelis and claiming that this was just the beginning of the OpIsrael campaign. On January 17, 2015 AnonGhost published an announcement regarding the defacement of the Web sites belonging to approximately 90 Israeli businesses. The announcement referred to various business sites as part of the OpIsrael campaign.[115]

On February 15, 2015 AnonGhost hacked the Web site of the State University of Ohio and dumped a list of 200 hacked domains, allowing access to said domains. The Center for Internet Security observed that AnonGhost had defaced 23 university Web sites as part of its recently announced OpChapelHill. The OpChapelHill campaign was in response to the shooting death of three Muslim students at UNC-Chapel Hill in February.

[109] https://twitter.com/RedHack_EN/status/562666341350801408
[110] http://www.zone-h.org/mirror/id/23400949?zh=3
[111] https://twitter.com/RedHack_EN/status/423233479673794560
[112] https://twitter.com/RedHack_EN/status/350606511837421568
[113] https://www.hackread.com/redhack-hacks-istanbul-police-assoc-website-berkin-elvan/ http://thecryptosphere.com/2015/03/12/redhack-strikes-back-at-police-on-the-anniversary-of-the-death-of-berkin-elvan/
[114] http://www.batblue.com/anonghost-declares-support-for-isis/
[115] http://pastebin.com/9qPFZkrX



#OpChapelHill
Hate Crime , Racism in US...
This Message Is Addressed To US Government
you have failed as expected
[illegible]
we will fight back !
[illegible]
We are AnonGhost
We are Everywhere
you should've Expected Us !

The message planted with a photo of the students killed on several defaced American Web sites

On March 3, 2015 AnonGhost hacked and defaced the official Web site of Colorado's Larimer County Sheriff's Office. The group left the following message on the site: "*This message is addressed to all governments...you have failed as expected…you can't stop the movement anymore…you can try to stop us, but we will always find a way to resist."* Aside from the defacement, the hackers did not do much else; no information or login credentials were stolen. There was no indication of a motive for the attack.[116] Two days later, AnonGhost again hacked the Web site of Colorado's Larimer Country Sheriff's Office and defaced the site with threatening messages. The message also stated that the government had failed its citizens. The Web site was shut down for several days as the issue was investigated.[117]

On March 7, 2015 AnonGhost defaced the official Web site of the state of Louisiana's Rapides Parish Police Jury, Southern Heritage Bank, and Churchill Banks. The defaced message read: "*We are watching you. Don't close your eyes…this message is addressed to all governments! For many years, we have witnessed your unjust laws. We will fight back! Expect us*!"[118]

[116] http://www.9news.com/story/news/local/2015/03/03/larimer-county-sheriffs-office-website-hacked/24330849/

[117] https://www.hackread.com/larimer-county-sheriffs-office-hacked-again/

[118] http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/anonghost-hacks-louisiana-websites/

Islamic Cyber Resistance

On December 13, 2014 an announcement was posted that claimed to have leaked the details of approximately 1,000 Saudi army and intelligence personnel that were registered for the HIS Jane's Defence Service.[119] The announcement,[120] which was published by Islamic Cyber Resistance, identified the operation with OpSaudi and with 'Anonymous', and listed names, countries, email addresses, places of work, job roles, etc.

On January 22, 2015 it was reported [121] that information was leaked from the official blog of PERL, which included details about approximately 2,500 users who were registered with the site.

OpFrance

Following the publication of a caricature of the Prophet Muhammad in the French magazine, *Charlie Hebdo*, in January 2015 and the terrorist attack at the magazine's offices, a Muslim hacker group carried out a series of breaches of French Web sites and defaced them. According to the daily, *Al-Arabi al-Jadid*, approximately 20,000 French Web sites have been breached and defaced since the terrorist attacks at *Charlie Hebdo*. The Tunisian Fallaga hacker group, for example, claimed responsibility for the breach of the *Charlie Hebdo* Web site and noted that it had gleaned from it a database containing sensitive material.[122] Hacking activities were mainly concentrated on the hashtag #OpFrance. For example, the Muslim hacker group, ANGOON, claimed to have defaced 500 French Web sites. [123]

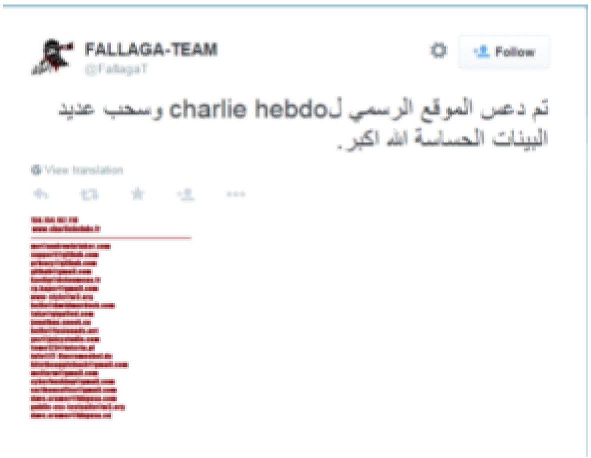
[119] http://www.janes.com/

[120] http://pastebin.com/bbGTndLB

[121] http://www.cyberwarnews.info/2014/01/22/official-perl-blogs-hacked-2924-author-credentials-leaked-by-icr/

[122] https://twitter.com/FallagaT/status/554587768320700416

[123] #OpFrance



FALLAGA-TEAM
@FallagaT

تم دعس الموقع الرسمي لcharlie hebdo وسحب عديد
البينات الحساسة الله اكبر.

The announcement by the Fallaga hacker group regarding the breach of the *Charlie Hebdo* site

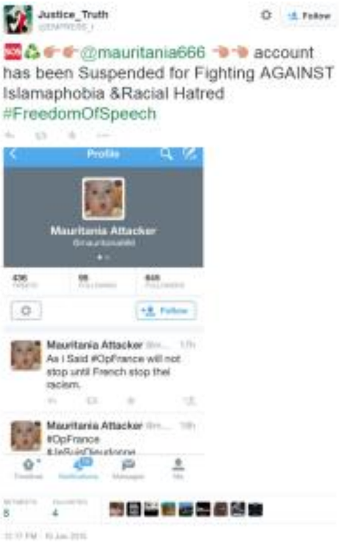
#OpFrance
AnonGhost
KHILAFA
I Am Muslim
and
I Am NOT
Charlie Pedo
Musulman et je suis pas charlie

A banner produced by the Muslim hacker group, AnonGhost, criticizing the *Charlie Hebdo* magazine

On January 16, 2015 it was reported that the Twitter account of a hacker known as 'Mauritania Attacker' was suspended. The hacker defaced many French Web sites in the framework of OpFrance,[124] and even published an announcement regarding an alleged attack on France's cellular network.[125]

The published announcement noted that the account was suspended:

[124] http://middleeasternet.com/?p=34554
[125] http://middleeasternet.com/?p=34648



Justice_Truth

🆘♻👉👉@mauritania666 👈👈 account has been Suspended for Fighting AGAINST Islamaphobia &Racial Hatred #FreedomOfSpeech

Profile

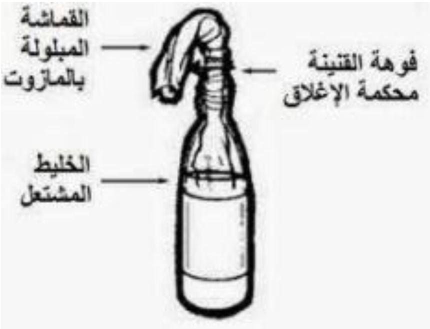
Mauritania Attacker

Mauritania Attacker
As I Said #OpFrance will not stop until French stop thei racism.

Mauritania Attacker
#OpFrance
#JeSuisDieudonné

5 4

In addition, many jihadists called on social networks to continue the wave of attacks on French soil, either as individuals or in small groups. For example, a virtual workshop opened on January 27, 2015 under the hashtag ورشة_عمل_الذئاب# (workshop of wolves), which was intended to help Muslims wanting to carry out spectacular individual attacks. For example, one visitor posted a guidebook on assembling Molotov cocktails to be thrown at Jewish and Western targets. In the framework of this discourse, correspondence was published encouraging lone wolf attacks.[126] One participant recommended hijacking an airplane and using it to get to the Caliphate territory.[127] Another visitor noted that if it is not possible to kill a soldier on French soil then one should burn businesses and churches.[128]



An illustration of a Molotov cocktail that was posted on Twitter

[126] http://justpaste.it/jihadi_3, #ورشة_عمل_الذئاب
[127] #ورشة_عمل_الذئاب
[128] https://twitter.com/Fatahmamo1/status/562633257037365248 . #الذئاب_المنفردة

Cyber-Crime and Cyber-Terrorism, January – March 2015

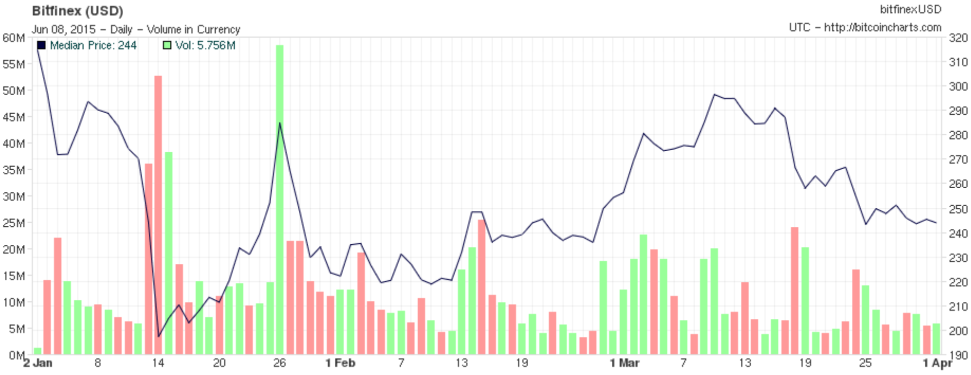
Recent years have seen an increasing number of cyber-attacks against political targets, critical infrastructure, and the Web sites of commercial corporations. These attacks, which are also receiving increasing amounts of international attention, are perpetrated by states (which do not take responsibility 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")[129] Internet between January - March 2015.

Virtual Currency

The below chart shows the Bitcoin price on the Bitfinex trading site for January - March 2015. During this period, trading in the amount of approximately 4.5 million BTC took place, at a value of over one billion dollars. The columns refer to the volume of the currency each day and the graph indicates the median price in American dollars on the same day.

At the beginning of this period, the value of Bitcoin was approximately $320 and by the end of this period dropped to approximately $245.

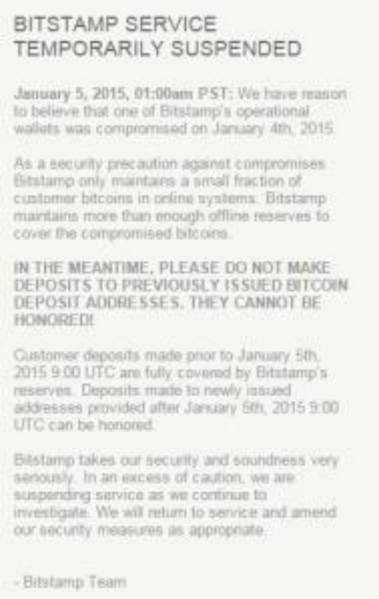
[129] The "dark Web" or darknet is "A collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks." See P. Biddle, P. England, M. Peinado and B. Willman (no date), "The Darknet and the Future of Content Distribution", *Microsoft Corporation*, http://msl1.mit.edu/ESD10/docs/darknet5.pdf.



Bitcoin price chart in Bitfinex for January - March 2015[130]

On January 5, 2015 an announcement was published on the virtual currency trading site, bitstamp.net, according to which the company has “reason to believe that one of Bitsstamp’s operational wallets was compromised on January 4, 2015”, and noted that as a security precaution only a small fraction of customer bitcoins were saved online.

Nevertheless, customers were instructed not to make deposits to accounts at this time, noting that deposits that were made by 09:00 UTC on January 5 were covered, in full, in the company reserves, as were the deposits made to new addresses after this deadline:



BITSTAMP SERVICE
TEMPORARILY SUSPENDED

January 5, 2015, 01:00am PST: We have reason to believe that one of Bitstamp's operational wallets was compromised on January 4th, 2015.

As a security precaution against compromises Bitstamp only maintains a small fraction of customer bitcoins in online systems. Bitstamp maintains more than enough offline reserves to cover the compromised bitcoins.

IN THE MEANTIME, PLEASE DO NOT MAKE DEPOSITS TO PREVIOUSLY ISSUED BITCOIN DEPOSIT ADDRESSES. THEY CANNOT BE HONORED!

Customer deposits made prior to January 5th, 2015 9:00 UTC are fully covered by Bitstamp's reserves. Deposits made to newly issued addresses provided after January 5th, 2015 9:00 UTC can be honored.

Bitstamp takes our security and soundness very seriously. In an excess of caution, we are suspending service as we continue to investigate. We will return to service and amend our security measures as appropriate.

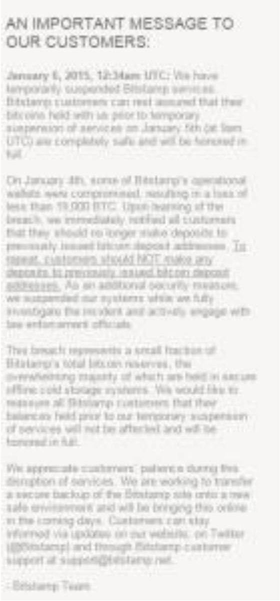
- Bitstamp Team

The next day, another, more serious, announcement was published indicating that the company

[130] http://bitcoincharts.com/charts/bitfinexUSD#rg60zczsg2015-01-01zeg2015-03-31ztgMzm1g10zm2g25zvzcv

was suspending all of its operations, while re-emphasizing that all actions taken up until the date noted in the previous announcement were secure and would be covered in full. Nevertheless, the announcement revealed that on January 4, approximately 19,000 bitcoins were stolen from the same operational account and that as soon as the breach was confirmed, a message was immediately sent to all customers not to make any further deposits to existing accounts.

It also stated that the company had suspended all of its systems during the investigation, which was being carried out in cooperation with law enforcement officials.



AN IMPORTANT MESSAGE TO OUR CUSTOMERS:

January 6, 2015, 12:34am UTC: We have temporarily suspended Bitstamp services. Bitstamp customers can rest assured that their bitcoins held with us prior to temporary suspension of services on January 5th (at 9am UTC) are completely safe and will be honored in full.

On January 4th, some of Bitstamp's operational wallets were compromised, resulting in a loss of less than 19,000 BTC. Upon learning of the breach, we immediately notified all customers that they should no longer make deposits to previously issued bitcoin deposit addresses. To repeat, customers should NOT make any deposits to previously issued bitcoin deposit addresses. As an additional security measure, we suspended our systems while we fully investigate the incident and actively engage with law enforcement officials.

This breach represents a small fraction of Bitstamp's total bitcoin reserves, the overwhelming majority of which are held in secure offline cold storage systems. We would like to reassure all Bitstamp customers that their balances held prior to our temporary suspension of services will not be affected and will be honored in full.

We appreciate customers' patience during this disruption of services. We are working to transfer a secure backup of the Bitstamp site onto a new safe environment and will be bringing this online in the coming days. Customers can stay informed via updates on our website, on Twitter (@Bitstamp) and through Bitstamp customer support at support@bitstamp.net.

- Bitstamp Team

On February 16, 2015 it was reported that 7,170 bitcoins worth approximately 1.7 million dollars were stolen from the Bter Chinese trading site.[131]

On February 17, 2015 the company CAVIRTEX, which provides virtual currency trading services, published an announcement[132] according to which it was immediately ending its trade in bitcoins and no new deposits would be accepted, trading would cease on March 20, and from March 25 no withdrawals would be made. The company added that it would contact every account holder to stop their activity following that date.

This took place two days after the company had discovered that an old version of its database,

[131] http://www.securityweek.com/7170-btc-stolen-chinese-bitcoin-exchange-bter
[132] https://www.cavirtex.com/news?page=2

including encrypted passwords, had apparently been breached despite its claim that the database did not contain identifying documents. For this reason, the company decided to stop existing activity in bitcoin transactions and return the money to all of its customers, maintaining that the damage caused to the company's reputation as a result of the breach would significantly impair its ability to continue operating this service successfully, and recommending that its customers change their passwords and clear the company's cookies from their browsers. Nevertheless, the company noted that it did not lose its customers' money and the production environment was not breached.

Two days later, another announcement was published according to which the company received a large number of positive responses since its initial announcement from governments, partners and community members. It also stated that customers would soon be able to make withdrawals of bitcoins and litecoins as a result of heightened security measures and the desire to verify that the account holder is indeed the one withdrawing the money. On February 23, a third announcement was published, which stated that bitcoin withdrawals had begun the previous week while the company examined the accounts following suspicious activity. Two days later, a fourth announcement was published according to which a phishing attack was being waged against the site's users via an executable file posing as a PDF file, enticing users to download the file by pretending to be a backup of the company's account authentication.[133]

On March 20, another announcement was published according to which all instructions were canceled and trading was stopped in accordance with the first message from February 17. The company appealed to all of its customers to enter their addresses in order to credit their accounts, claiming that this information was erased during the month of February. Finally, on March 24, the last announcement was published according to which withdrawals would continue via direct deposit of bitcoins and litecoins until April 1, in contrast to the previous announcement that stated that withdrawals would stop on March 25. It further stated that the company was no longer processing trade transactions.

On March 18, an announcement was published regarding a beach of the AllCrypt trading site in which 37 bitcoins were stolen.[134]

[133] https://www.cavirtex.com/news?page=2

[134] https://archive.is/2UY7e

Developments in International Legal Efforts to Combat Terrorism in Cyberspace

The United Nations Security Council has stepped up its efforts to engage Member States in a variety of measures to combat terrorism over the past few months, in particular to mitigate the increased use of cyberspace by extremist groups in the Middle East.

Three resolutions in particular exemplify this new approach, noted under the category of "Threats to peace and security caused by terrorist acts" and prompted by acts of terrorism and their promotion via the internet by the Islamic State, Al-Nusra Front, Al-Qaeda and similar terrorist groups. These are Resolutions 2170 (August 15, 2014), 2178 (September 24, 2014) and 2199 (February 12, 2015).

This recent series of resolutions, taken under the Charter's Chapter VII, represent the Security Council's awareness of the need to prevent the use of the Internet by extremist groups to recruit members, fund terrorist activities, propagandize, and otherwise leverage the internet and social media at an unprecedented global level. These issues characterize terrorists' exploitation of new communications technologies, as distinct from the use of cyberspace, to commit actual acts of terrorism such as attacks on critical infrastructure with physical, real-world consequences.

Resolution 2170 notes the Security Council's motivation in one of its opening paragraphs:

> *Expressing concern* at the increased use, in a globalized society, by terrorists and their supporters of new information and communication technologies, in particular the Internet, for the purposes of recruitment and incitement to commit terrorist acts, as well as for the financing, planning and preparation of their activities, and underlining the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law…

While there is at least one precedent for the Security Council to note terrorists' use of Information and communications technology (ICT) in its resolutions (in the context of Angola's UNITA), the Council has significantly expanded its Chapter VII requirements of Member States to cooperate on the exchange of information on terrorist use of the internet through shared data on internet communications, social media and electronic databases. This includes, but is not restricted to, data such as international travel data and airline passenger data. See, for example, paragraph 11 of UNSC 2178:

> Acting under Chapter VII of the Charter of the United Nations….

> [The UN Security Council] [c]alls upon Member States to improve international, regional, and subregional cooperation…to prevent the travel of foreign terrorist fighters from or through their territories, including through increased sharing of information for the purpose of identifying foreign terrorist fighters, the sharing and adoption of best practices, and improved understanding of the patterns of travel by foreign terrorist fighters, and for Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts…

Finally, the Security Council has urged Member States to take measures to prevent terrorist exploitation of social media such as YouTube, Facebook and Twitter. Paragraph 17 of Resolution 2178 specifically requires them *"…to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources, including audio and video, to incite support for terrorist acts…"*

While some Member States have begun efforts to implement the substance of these and other similar resolutions, in their domestic legislation – France is one example – the extent to which UN members will cooperate in order to bring them into effect is still evolving.

In conjunction with these efforts of the Security Council, other international consortia, such as the UN's Counter-Terrorism Implementation Task Force's Working Group on Countering the Use of the Internet for Terrorist Purposes and the Global Counterterrorism Forum, are developing specific strategies for countering terrorist use of the internet.

Broader concerns of the maintenance in cyberspace of the rule of law - and in particular individual privacy, the freedom of communication, and other human rights - are engaging states in this context.

How the US Financial System is Facing Cyber Challenges and Threats

On March 17, 2015 the Federal Financial Institutions Examination Council (FFIEC) announced[135] its intention to take several additional steps in order to help banking institutions cope with cybersecurity risks.

In this framework, they will update its Information Technology Examination Handbook in order *"to reflect rapidly evolving cyber threats and vulnerabilities with a focus on risk management and*

[135] https://www.ffiec.gov/press/pr031715.htm

oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and incident management and resilience". However, it did not state when the new cybersecurity policy would be implemented.

It also revealed six more key measures;

Cybersecurity Self-Assessment Tool – The FFIEC intends to produce such a tool during the year in order to help institutions evaluate their cybersecurity risks and their risk management abilities.

Incident Analysis – FFIEC members will improve the processes for collecting, analyzing and sharing information with one another during cyber incidents.

Crisis Management – The FFIEC will arrange, update and examine protocols for an emergency as a response to large-scale cyber incidents, while coordinating with public and private partners.

Training – The FFIEC will develop training programs for its members' staff on the issues of cyber threats and vulnerabilities.

Technology Service Provider Strategy – FFIEC members will expand their activities concerning the ability of technology service providers to respond to cyber threats and vulnerabilities.

Collaboration with Law Enforcement and Intelligence Agencies – The FFIEC will expand its collaboration with law enforcement and intelligence agencies in order to share information on growing threats to cybersecurity and response methods.

Crime in the Medical Arena

In January 2015, the medical insurance company, Anthem, announced that its systems had been breached. Here too, the media revealed that there is a risk that 78.8 million of the company's customers were leaked.[136] On March 16, Sacred Heart Health System announced that information about 14,000 customers was leaked in the beginning of February.[137] On March 17, Premera Blue Cross announced [138] that it was the target of a sophisticated cyber-attack during which the attackers managed to gain access to the company's information systems, which led them to reveal the personal information of its customers.

The company announced that it would provide its customers with free access for two years to

[136] http://abcnews.go.com/Technology/anthem-hack-impacted-millions-customers/story?id=29212840
[137] http://www.sacred-heart.org/news/article/?NID=1832
[138] http://premeranews.com/2015/03/17/cyberattack-information-for-premera-members/

credit monitoring services and identity protection by the company, Experian, including constant updating for those affected by this breach. For this purpose, the company even created a special Web site with additional information for its customers. An examination of this site indicated that the company was made aware of the attack on January 29, 2015, and that tests revealed that the first attack had taken place on May 5, 2014, as well as the fact that the stolen information may have dated back to 2002. The announcement stated that the company took measures to protect and support its customers who were affected - and involved the FBI in the company's investigation of the cyber-security incident, which it carried out in cooperation with the company, Mandiant - as well as to clean its systems of the ramifications of the breach and improve the security of the information systems.

The announcement explained that:

> "The attackers may have gained access to the personal information of our members, along with the information of our employer customers, healthcare providers and other people and organizations with whom we do business. That information could include names, dates of birth, addresses, telephone numbers, email addresses, Social Security numbers, member identification number, medical claims information and financial information. It's important to note that our investigation has not determined that data was removed from our systems. We have no evidence at this point that any of the data that may have been accessed during this attack has been used inappropriately."

Medical insurance companies and hospitals are turning into preferred targets for hackers since their computer systems contain not only personal information and credit card details, but also medical information about the customers of these companies – valuable information for various entities.

The illegal trade in medical information is on the rise and very profitable, with information about ten people selling for 10 bitcoins, more expensive than credit card details or personal details used for the purpose of identity theft. [139]

Online Fraud – The Dark Side of the Internet

The relative anonymity provided by the Internet, as well as its broad distribution, immediacy and

[139] http://www.npr.org/blogs/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data?linkId=12349724

access to information from a wide range of devices, creates threats and risks along with advantages and opportunities. An example of this is online fraud carried out by criminal elements who recognize the great potential and relative ease of these scams as compared to scams in the physical world.

These scams are carried out against individuals, small businesses and huge companies in the form of targeted phishing attacks against pre-selected targets, and in the form of network-wide deployment in the hopes of ensnaring as many victims as possible.

There are cases of fraud in which criminals impersonate large companies and send an email, seemingly from the company and sometimes using the user's real name as a personal reference. The email either contains intriguing content, such as the arrival of a package or confirmation of a hotel reservation, [140] or threatening content, such as a hold on a customer's account or credit card.[141] These messages contain infected files that, upon being opened, enable the sender to gather sensitive information, including passwords, from the computer and transfer them to a remote server without the user's knowledge. The messages may also contain links to seemingly authentic Web pages in which the user is asked to enter a username and password[142] without knowing that the page is fake and that he is providing these details to cyber criminals.

Most of these cases are characterized by the ease with which it is possible to defraud the consumer and Internet user in this digital age of online communication. Therefore, users of the Internet, social networks and digital payment tools must be more aware and conscious of the risks involved, and adopt the same precautions that we are used to taking in the physical world but do not necessarily take in this changing and developing digital world.

Malware Ransom

The industry of malware ransom continues to thrive. According to Dell SecureWorks, malware named CryptoWall struck approximately 600,000 computers during the first half of 2014 and gained approximately one million dollars from various users who paid a ransom of $100-$500.[143] Another

[140] http://www.ibtimes.co.uk/hotel-website-booking-com-targeted-by-phishing-scammers-1473822
[141] https://blog.sucuri.net/2014/12/targeted-phishing-against-godaddy-customers.html
[142] http://middleeasternet.com/?p=31910
[143] http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/

malware that mainly operated in Australia named TorrentLocker earned approximately 200,000 dollars in revenue per month.[144] In mid-March, a new ransom malware was reported named TeslaCrypt that, in contrast to other malware, encrypts computer game files.[145]

The ransomware message - in which the user receives an email requiring him to pay a certain amount of money or else his Internet activity will be blocked, or in order to release blocked computer files - presents not only a technological challenge and risk, but an emotional and human one as well.

Joseph Edwards, a 17-year-old high school student from Britain, hanged himself after he received a disturbing email message that pretended to be from the police, according to which he had been seen using illegal Web sites and, therefore, had to pay a fine of 100 pounds in order to avoid prosecution. The teen, who was developmentally disabled, believed that the message he received was original and had indeed come from the police. This affected him emotionally to the point that he chose to hang himself several hours after receiving the email.[146]

The Fight against Terrorism on the Internet

British Prime Minister, David Cameron, claimed in the beginning of January that the legislation must be changed to enable intelligence agencies to decrypt the communications of terrorism suspects. This report came after EU ministers demanded that social media sites increase their cooperation in preventing jihadists and terrorist organizations from using the Internet for recruitment and propaganda purposes. [147]

In the beginning of February, the White House announced the establishment of a new agency called the Cyber Threat Intelligence Integration Center to combat cyber threats based on the National Center for Combating Terrorism. [148] In March, the Senate Intelligence Committee raised the issue of

[144] http://news.softpedia.com/news/TorrentLocker-Operators-Make-About-224-000-In-About-A-Month-469680.shtml
[145] https://blogs.mcafee.com/mcafee-labs/teslacrypt-joins-ransomware-field
[146] http://thehackernews.com/2015/01/police-ransomware-suicide.html
[147] http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg
[148] http://www.washingtonpost.com/world/national-security/white-house-to-create-national-center-to-counter-cyberspace-intrusions/2015/02/09/a312201e-afd0-11e4-827f-93f454140e2b_story.html

the reporting obligation per the Cybersecurity Information Sharing Act.[149] On March 1, it was published that Saudi Arabia intends to establish an international coalition in order to combat Web sites that support and encourage terrorism.[150]

The Secretary-General of the International Commission for Technological Means, Ali al-Obeidi, stated that that goal is to investigate Web sites that support terrorism and keep them away from the public before the month of Ramadan (which began this year on June 18), and for this reason the Commission has begun to establish alliances with governments and research centers within and outside Saudi Arabia, including Kuwait, Malaysia and Egypt. According to him, the goal of the Commission is "to correct the erroneous knowledge about Islam by exposing the cunning ways used by terrorists to attract newcomers via the Internet".

Saudi Arabia has been combating Internet content for years, both for moral considerations and as part of the fight against terrorism in the country. In this framework, it was reported that over 10,000 Twitter accounts in the Kingdom were shut down during 2014 due to "religious violations",[151] in addition to reports [152] in October 2014 that the Ministry of Culture of Information intended to impose regulations on Web sites for sharing photos or videos in order to guarantee that they operate in accordance with the laws of the Kingdom.

In addition, as part of the war on terrorism in its country, government officials in the Kingdom already addressed [153] back in 2011 the ease of illegal online weapons trading as well as the battle against the phenomenon of illegal trading in SIM cards, which enables the anonymous purchase of these cards by terrorists.[154]

In this context, it was published on the Egyptian news site, Ahram Online,[155] on February 17 that the Egyptian Prime Minister had announced the establishment of a committee "to investigate possible amendments to national security laws in order to remove terrorism-related Web sites". The Cabinet spokesman stated that the recommendation of the committee, which will be headed by the Justice

[149] http://www.washingtonexaminer.com/liability-protection-will-be-the-key-to-any-information-sharing-bill/article/2561107
[150] http://www.albawabaeg.com/51239
[151] http://www.arabnews.com/news/674696
[152] http://www.arabnews.com/saudi-arabia/news/651306
[153] http://www.aleqt.com/2011/09/05/article_576582.html
[154] http://www.arabnews.com/news/538256
[155] http://english.ahram.org.eg/News/123290.aspx

Minister and should begin to operate soon, will help the courts to rule in favor of removing all terrorism-related content. The committee will also be composed of representatives from the Ministries of Interior, Defense, Military Production, Foreign Affairs and Communications. However, according to him, it has not yet been determined which characteristics the committee will use to determine if a Web site's content is related to terrorism or not.

In addition to the physical terrorist activities carried out by the IS throughout the Middle East, the organization also carries out online activities that know no borders and can reach every home around the world. As part of the battle against such online activity, a court in Vienna sentenced a 20-year-old Kurdish man to a six-month suspended sentence for posting IS propaganda [156] on Facebook as well as photos of the organization's horrific actions on his Facebook page. The young man was caught together with 12 others in a police raid at the end of November 2014, including an Islamic preacher who led a group in the city called "The Bosnian cell" and who was accused of recruiting fighters to the ranks of the IS in Syria. At his trial, the young man said that he was born in Iraq and had no connection to religion until the age of 15-16 when he changed his ways and turned to religion and prayer, and he claimed that posting the photos was "real stupidity". However, the judge was not swayed by his words and sentenced him to a six-month suspended sentence but due to his lack of a criminal record he was sentenced to probation and three years' probation.

Case Study – #OpIsrael - AnonGhost[157]

Each newsletter issued by the ICT's cyber-desk will discuss in greater detail a recent incident of cyber-attack.

From security to defense –changes in offensive and defensive strategies in the fight against cyber-terrorism. Which of them are more effective and why?

On April 7, 2013 the group 'Anonymous' launched its first cyber-attack against Israeli Web sites under the name #OpIsrael. This attack has been repeated every year on the same date with minor differences – each year different attack techniques are used, organizations in Israel use different security responses, and the results of the attack change accordingly.

The history of this series of attacks reflects the changes and the varying trends of cyber-attacks over

[156] http://www.thelocal.at/20150226/six-months-for-isis-facebook-postings

[157] Written by Eli Amar.

the years, as well as the evolution of the security actions taken to combat them. What has changed in terms of the attacks over the last two years, why have they become less severe, and what does this teach us about information security?

According to members of ‘Anonymous’, the attacks are aimed at damaging the State of Israel’s information infrastructure and even its stable lifestyle. Group members declare their desire “to wipe Israel off the Internet” due to claims of its crimes against Palestinians. The cyber-attacks are carried out by hackers who identify themselves as Arab and Muslim activists affiliated with ‘Anonymous’, which includes members from around the world.

The first attack, which took place in 2013, was mainly an attack on the Internet infrastructure in Israel. Among other things, DDoS attacks were carried out against DNS servers in “denial of service” attacks. This type of attack is carried out remotely and is based on overloading the servers of a specific service until they crash. Some DDoS attacks were directed at Israeli Internet bandwidth providers by utilizing the bandwidth to the point of disrupting network usage at a volume that reached tens of gigabytes per second.

In addition to the DDos attacks, the group also carried out breaches and attacks with the aim of defacing Web sites identified as Israeli, in both the government and civilian sectors, and even breached sites belonging to private businesses. The goal of the attackers was partly achieved – several essential government services were not available for several hours and various sites were partially damaged, including the Web site of Yad Vashem, which reported a heavier than usual load but was still available – and news sites reported glitches.

In the framework of the 2014 attacks, most of the effort was again focused on the civilian sector and reports of overloaded bandwidths of Israeli providers were again noted. This time, the attack was carried out against NTP or DNS servers, two different protocols that are frequently attacked. These protocols are configured on the home router – in other words, at the client’s home - which belongs to the civilian sector. So, technically speaking, the attack reached the entrance of the customer’s home and was not directed at the provider. These attacks were successfully stopped by the providers but hampered the availability of several essential civilian services, and Web sites in the civilian and government sectors crashed, including the site of the Central Bureau of Statistics.

However, the picture changed with the third attack. In 2015, DDoS attacks were again carried out but this time most of them were blocked. Several private sites were defaced, including the site of the Meretz Party, the official site of singer Shalom Hanoch, and the site of the Papagaio restaurant chain. Nevertheless, general speaking, all of the “denial of service” attacks failed, government Web sites continued to operate, and most of the attacks on the civilian sector were blocked, such that the cyber-attack did not end with dramatic results.

What changed between 2013-2015 that led to the successful obstruction of cyber-attacks and what can be learned about the evolution of cyber-terrorism and the defenses against it?

First of all, the various attacks were not blocked as a result of the technology or infrastructure through which the attack was carried out, so the differences were not dependent on technological reasons of infrastructure development. There were no special changes to the various levels of regulation: the guidelines relating to the security of the country’s critical systems, such as Internet providers, remained fundamentally unchanged. Even the Israel Internet Association, which operates not-for-profit for the good of the Israeli public and, among other things, for Internet stability in the country, did not issue new guidelines and itself was even a target of previous attacks by ‘Anonymous’. Even according to the Ministry of Communications, no new guidelines were issued prior to the event. Why then were most of the attacks blocked?

The answer has to do with the level of responsibility expected of the service providers. Between 2013-2015, in the framework of internal investigations that were carried out in the services and infrastructures sector, the level of involvement and the level of exposure of civilian entities increased significantly. As a result, the level of responsibility expected of Internet service providers increased: the perception of service providers as ‘service oriented’ and providing a collection of individual services changed to a perception of them as ‘service expected’ according to which they were forced to adapt themselves to the services expected of them by their customers. At the same time there was an increase in local initiatives by security companies that received a stream of information about events, and collaboration began to take shape between the private and government sectors, and those responsible for essential infrastructure. Infrastructure providers, which are now viewed as the body responsible for the availability of essential services, began to see their clients themselves as an unknowingly “potential threat” due to the use of protocols such as NTP and DNS, which are configured in the client’s router, in cyber-attacks. Internet service providers were forced to guard themselves against both external and “internal” threats, in the form of their customers, and began to enforce a defense policies as opposed to security policies.

The difference between defense policies and security policies lies in where the organization invests its efforts: with security, the effort is invested in protecting the company's assets solely within the organization. In contrast, with defense, barriers are also constructed at the customer level and with all branches of the organization's activities. This trend is not unique to Israel and can be seen in trends around the world: a document published by NATO on the topic of security against cyber-attacks pointed out that all over the world there is a transition taking place from security policies to defense policies against cyber-attacks. The greatest change is taking place in the United States where a shift has started to take place in the general perception relating to security and cooperation. Today in the US there is a body that deals with cyber-attacks and wide collaboration between the industrial and government sectors, as well as the establishment of value-added services for the public. There is no doubt that these changes reflect the understanding that cyber-terrorism is a real threat to infrastructure that is liable to result in damage to the country's institutions as well to the private sector, and therefore many diverse organizations have a clear interest in protecting themselves.

Significant changes have also begun to take place in Israel in terms of its security policy against cyber-attacks. This policy was implemented in three steps:

1. Cooperation – the creation of a large-scale information sharing between various bodies - starting with the Israel Internet Association, which established a situation room that operates regularly, to special situation rooms that are operated by volunteers on the day of the event and manned by cyber-security expert advisors in Israel. All of the information accumulated in these situation rooms was available to anyone who requested it.
2. Personal Responsibility – responsibility for security at the customer level. For instance, when a customer purchases services from a server farm, whether it is only used as a server locally or on the ground floor, the customer must abide by a number of laws relating to security. These laws protect the rest of the sites hosted on the same server farm.
3. Operational Responsibility – Today, providers are defined as entities that provide the most critical infrastructure for the Israeli economy. As such, they take part in information sharing, both as information gathering initiatives and as information recipients. The level of cooperation is also gaining momentum within sectors, such as the banking sector, the transportation sector and the industrial sector. Mandatory information sharing essentially

provides a window of time to create a timely defense: by reporting an attack on one Web site, the information helps to block an attack somewhere else.

Indeed, not everything is rosy and there is room for improvement both at the policy making level and the policy implementation level, but the fact cannot be ignored that in the framework of the three most recent cyber-attacks carried out by 'Anonymous' against Israel, the level of damage to infrastructure has declined.

So what is missing in order to complete the picture and create optimal security? We propose three channels for advancing the level of security in the country:

1. The integration of research, development and intelligence bodies, such as the National Cyber Headquarters, in order to supply and transmit information to all those who seek it – from local companies in small cities to providers or large companies.
2. Determination of a body to deal with the event. This topic is especially important during a "on going" attack: for instance, a situation that begins with a small company in the city of Metula that hosted its Web site with a local provider can develop into an event that results in the defacement of hundreds and thousands of information assets of various companies and can even result in the crashing of the main artery. In such a case, a decision must be made as to how to handle the event: Does every company bring in its own experts? Who conducts the coordination in an event affecting several sectors?
3. Creation and strengthening of synergy and interaction within each sector. For example, one can look at the banking industry, which established the Financial Services Information Sharing and Analysis Center (FS-ISAC). The Center is responsible for the gathering and analysis of information between international organizations. However, in order to make advance warning information effective, there must be integration of the information in practice and at the process level in the local market.

Today it is clear that the civilian market cannot cope alone with attacks by hostile factors at the level of a state, a terrorist organization or an activist group. In order to ensure the immunity of the civilian market, additional changes must be made based on insights regarding cooperation, available information, and an integration of information in the local market. Such initial insights can be seen in the transition from an internal security outlook to a defense outlook that includes the customer and external circles, in incidents of information sharing, and in the joining of response teams, which are already affecting the immunity of the sector and contributing to its defense. Continued activity according to these insights will ensure continuous improvement to security against cyber-attacks; security that is an interest of the civilian market as well as of the government bodies responsible for infrastructure protection.

ICT Cyber-Desk Team

Dr. Eitan Azani, Deputy Executive Director, ICT

Eli Amar, Expert on Cyber Security, EA Cyber

Dr. Michael Barak, Team Research Manager, ICT

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

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

Shuki Peleg, Information Security and Cyber-Security Consultant

Nir Tordjman, Team Research Manager, ICT

ICT Interns

Chantelle Berman

Efrat Eckstein

Riana Goren

Kathryn Johnston

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.