IDC HERZLIYA

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

ICT Cyber-Desk

PERIODIC REVIEW

Cyber-Terrorism Activities

Report No. 13

April – June 2015

Highlights

This report covers the period of April - June 2015 and addresses two main subjects: cyber-terrorism (offensive, defensive, in the media, and the main topics of jihadist discourse) and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack).

The following are among the issues covered in this report:

- The issue of anonymity and encryption continues to be at the forefront of discussion topics on forums, with the goal of increasing security levels of users, and preventing exposure and identification of the security mechanisms. It is possible to differentiate between guides for secure and correct internet use, and recommendations for using free programs and services incorporating technologies that include high levels of encryption and anonymity. Some of the recommendations relate to information encryption on computers or mobile devices, including cellular phones and tablets.
- There has been in increase in groups affiliated with the Islamic state, such as the IS Cyber Caliphate Hacking Division and the ISIS Cyber Army. There are also known hacker groups which have only recently started identifying with IS activities – for example, groups from North Africa, and in particular Morocco. There has been a noticeable increase in Muslim groups that have changed their messages, as they have begun attacks such as websites defacements, while beginning to exhibit characteristics which indicate their support for the Islamic State. In addition, there is an increase of significant threats of cyber attacks on Western targets – specifically the United States - by groups affiliated with the Islamic State. It should be noted that most of the known attacks have been directed towards small websites with minimal security levels, and that no attack caused significant damage. However, there were also several significant attacks, such as the one on the French television channel, TV5 Monde. In addition, attempts to leak classified data by breaking into government sites has been observed. It is estimated that in some of the cases, the documents publicized were already available to the public on the internet.
- Incidents of data and information leaks increased in number, and in the scope of information that was stolen and leaked. An increase in theft incidents which were carried out as Cyber crimes has also become discernible, though there still a differentiation between hacking for personal data, financial information (including credit card details), medical information, and

commercial information. Among the more significant attacks was the hack into the Office of Personnel Management and the theft of private details of millions of US government employees. In a large number of the attacks, the scope of information stolen relates to millions of users, while part of the information, such as financial or medical data, was sold on the black market and to forums on the Dark Internet. Personal information was sold for use in future attacks, including blackmail and phishing attacks.

- Many countries are intensifying their investments and preparations for coping with threats to cyberspace – whether by amending laws or establishing institutions and authorities with the authorization and responsibility for coping with these challenges.
- Over the past few months, the United Nations Security Council has stepped up its efforts to engage Member States in a variety of measures to combat terrorism, and in particular to mitigate the increased use of cyberspace by extremist groups in the Middle East.
- This report includes a case study of the OpIsrael 2015 campaign, which reached its climax on April 7. Different hacker groups took part in the attack, such as Anonymous Arabe, AnonGhost, and others.

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 noteworthy acts of electronic jihad, and a brief overview of the key themes reflected in jihadist discourse and propaganda.

Key Topics of Jihadist Discourse, April - June 2015

The Al-Qaeda Organization

A series of assassinations of senior jihadist leaders in branches of Al-Qaeda in the beginning of April often came up in jihadist discourse. Al-Qaeda in the Arabian Peninsula offered words of eulogy in memory of Sheikh Ibrahim al-Rubaysh and Sheikh Nasr al Anisi, a mufti and a leader of the organization, respectively, who were killed by American drone fire. Al-Qaeda in the Indian Subcontinent also issued words of eulogy in memory of two of its senior leaders, Sheikh Ahmad Faruq, deputy leader of the organization, and Al-Qari Amran, a member of the Shura Council, who were killed by American drone fire in January 2015. As a result of the assassination of al-Anisi, Qasim al Raymi - the new leader of AQAP - pledged allegiance to Sheikh Ayman al-Zawahiri. The internal jihadi controversy going on between the different Al-Qaeda factions and the Islamic State, continued to occupy the jihadist discourse from April through June. For example, Sheikh Abu Muhammad al-Adani, spokesperson for the Islamic State, stated that the shari'a laws should be implemented as religious law, but only within territories under the authority of the Islamic State. In response, Sheik Abu Muhammad al-Maqdisi, a senior Salafi jihadist philosopher in Jordan who supports Al-Qaeda, commented that the shari'a laws should also be implemented as religious law in areas controlled by the Taliban and other jihadist organizations, such as the Al-Nusra Front. Also, the Islamic State doesn't truly implement the shari'a laws, because it executes people for reasons that go against shari'a law, and fights against other jihadist organizations. Concurrent to this

criticism, al-Maqdisi emphasized that it is forbidden to fight against members of the Islamic State, except in cases of self-defence.

Deputy head of the Afghan Taliban organization, Akhtar Mohammad Mansour, also expressed his dissatisfaction over the way the Islamic State conducted itself when interacting with other jihadist organizations, and demanded of Abu Bakr al-Baghdadi, leader of the Islamic State, to fight under the auspices of the Afghan Taliban, and to try to end the rift between the jihad fighters.

Al-Nusra Front

The success of the jihadist organizations - led by the Al-Nusra Front - in liberating Idlib Province in Syria, is a popular topic of jihadist discourse in the period being covered. Abu Bakr al-Julani, leader of Al-Nusra Front – a branch of Al-Qaeda in Syria – sent his blessings to the fighters of that organization and to other jihadist organizations, such as Ahrar Al-Sham, which took part in the liberation of Idlib Province from the clutches of the Syrian regime. According to al-Julani, the best way to control the liberated province will be by means of a Shura Council, as well as by maintaining unity among the ranks. In addition, al-Julani called upon the Muslim residents of other Syrian cities to support jihad and to wait patiently for their liberation. In response to the military achievement, Abu Musab Wadoud, Emir of Al-Qaeda in the Islamic Maghreb, sent blessings to the jihad fighters in Syria and emphasized the importance of maintaining unity among the ranks, and on focusing on the implementation of shari'a.

The Islamic State

The Islamic State continued to bolster its public relations campaign and its recruitment of Muslims from other countries, such as Saudi Arabia and Somalia. Thus, for example, it claimed responsibility for a suicide attack it carried out against a Shi'ite prayer sanctuary in Eastern Saudi Arabia, and in Kuwait. It called upon Muslims in Somalia to join IS ranks, called upon Muslims in Tunisia to join jihad in Libya, and called upon Sunni tribes in Yemen to fight against the Houthis, while simultaneously calling upon the jihadist organizations in Yemen to dismantle and pledge allegiance to the Islamic State.

In addition, the Islamic State trend of employing terror as a form of psychological warfare continues to prevail. For example, the Islamic State executed about 30 Christian Ethiopians who

were residing in Libya. In addition, the IS threatened to continue its policy of executions with dozens of Kurdish Peshmerga fighters, if they didn't stop battling against the Islamic State fighters. The IS also claimed responsibility for a June 26 terror attack by its fighters, who opened fire on tourists on the beach and in a hotel compound in the vacation town of Sousse. According to the organization, the attack on the tourists was justified because they were citizens of the coalition countries that attacked the Islamic State.

Another prominent issue in the jihadist discourse revolves around IS taking control of about 80% of the territory in the Al-Yarmouk Palestinian refugee camp in Syria. According to IS fighters, the conquest of the camp successfully "thwarted" the plans of jihadist factions loyal to Assad to hand the camp over to him. That was while rivals of the IS, such as Hamas, claimed that occupying the camp caused a severe humanitarian crisis.

Al-Shabaab Al-Mujahideen

Al-Shabaab Al-Mujahideen in Somalia threatened to carry out terror attacks against Kenyan civilians, in revenge for the methodological "massacre" of the Muslim population in East Africa – and in particular in Somalia – by the Kenyan government. At the same time, **Al-Muhajiroun in East Africa**, affiliated with Al-Shabaab Al-Mujahideen, threatened to unleash a wave of terror attacks against Tunisia, Uganda, and Kenya. According to the organization, it intended to collapse the national borders created by colonial forces in East Africa, through cooperation with the Somali Al-Shabaab organization and Al-Qaeda.

Al-Qaeda in the Islamic Maghreb

Al-Qaeda in the Islamic Maghreb called upon the Tunisian people to continue rebelling with jihad, claiming that the present regime had not been changed, and that the old "tyrants" had simply been replaced with new ones. According to the organization, a desire to return Islam to Tunisia without harming innocent people was apparent. In addition, the organization addressed fighters from the Uqbah bin Nafi Brigade in Tunisia, praising their jihadist war, but also warning them not to transform into mercenaries.

Jihadist Propaganda

- A new jihadist forum was launched, called "The Technological People of The Caliphate State",

which identifies with the Islamic State. The forum is mainly devoted to cyber and internet topics, and contains guides, advice, and articles on subjects such as hacking, safe surfing on the internet, and more. In addition, the forum publishes videos and official statements of the Islamic State.[1]

The new forum's banner

- A poster on the Arin Al-Mujahideen forum, Abu Qatada al-Salafi, publicized the opening of a Twitter account by the Al-Qaeda media institution. The account was called "Al-Hikma Al-'Ilamiyya" instead of the organization's former Twitter account, which was called "Al-Hussam Al-'Ilamiyya". According to the statement, the change took place because the manager of the previous account had collaborated with the Saudis and the West. According to the post, the new media institution would have two Twitter accounts. The first, ALHKMA_1@ would publish Al-Qaeda's official statements, and in the second, ALHKMA_2@, unofficial tweets would appear. In addition, according to the announcement, anyone who wanted to post on the Twitter accounts could make contact with the manager of the Twitter account, Abu Kaysar al-Ansari, at the address mojahadYEeo5@.[2]

Defensive Tactics

The subject of anonymity and encryption continued to be the focus of discourse in forums, with the goals of increasing the security levels of users, and of preventing exposure and identification of the security mechanisms. It was possible to differentiate between guidebooks for safe and correct use, and suggestions for using programs and free services that work with technologies that include encryption and anonymity levels. Some of the recommendations related to security for transferring information as part of internet use of, and the rest of the

[1] http://www.s3cur1ty-is.com/vb/
[2] https://al-aren.com/vb/

recommendations related to stored information encryption, whether on a computer or mobile device, including both cell phones and tablets.

- A prominent poster called "The Technology Man of the Islamic State" (Tikni al-Dawla al-Islamiya) published during the months April through June 2015 several guides and publications on the subject of safe internet surfing:
    - The Technological Man of the Islamic State published a broad explanation about the way the "Tails" program – an anonymous operating system – is installed. The official name of the program is "Amnesiac Incognito Live System". After installing the operating system, which is based on Linux from a DVD player, an SD card, or USB memory, it is possible to surf the internet without leaving any tracks (unless specific instructions are given otherwise). The operating system includes tools for encryption and protecting privacy, and an internet browser that uses TOR technology, a program for immediate messaging, an email customer, and tools for editing images and sounds.[3]

The Tails logo

    - A series of old and new lessons about cell phone security, including: using applications on an android phone in a manner that prevents the leakage of personal details about the phone's owner, an explanation about how to use ORBOT (an encryption program for cellular phones), a recommended security program to download on I-phones and androids, an explanation about how to encrypt android phones, ways to avoid using services like Google on androids, and more.[4]
    - A series of old and new lessons about securing personal computers, including: how to install the Kaspersky anti-virus program on a Windows operating system, how to surf

[3] https://dump.to/TAILS
[4] https://dump.to/ARCHIVE1

safely using the TOR encryption program, how to protect a computer for Keylogger[5] for Windows, how to encrypt files using the VeraCrypt[6] program, encrypting a USB, and more.[7]

- A guide for installing and using encrypted email programs, called proton mail, TUTANOTA, and HUSHMAIL.[8]

Logos of encrypted email programs

- A guide in English about how to ensure information security on a Smartphone.[9]
- A series of articles called "The Electronic War and the Disregard Shown by Supporters of the Islamic State" – a series of articles mainly based on leaks made by Edward Snowden. Snowden is an American citizen who worked for the American Central Intelligence Agency until 2013, when he defected to Russia after leaking sensitive information about cyber spying by the agency. The purpose of the articles was to bring to the attention of internet users security and safety rules which should be followed when surfing on the net.[10]

[5] Malware that monitors keyboard action on a device
[6] A program that encrypts the data found on a drive
[7] https://dump.to/windowssec
[8] https://dump.to/Emailencrypted
[9] https://dump.to/protecotionISO2
[10] https://dump.to/cyberwarfare

Edward Snowden

- Athir Al-Madina – a branch of Ansar Al-Sharia in Libya, announced it would begin using the program TELEGRAM for sending encrypted messages to cellular phones. In addition, it publicized a phone number for contacting the organization.[11]

Website banner

- The Salafi Army of the Nation in Jerusalem, published internet safety guidelines for activists and media people in the Gaza Strip. The guidelines were taken from the Cyberkov website: https://blog.cyberkov.com/1814.html.[12]
- A visitor to the jihadist forum Shumukh al-Islam published a detailed explanation, accompanied

[11] https://twitter.com/AtherMadina/status/594498449292288000
[12] https://al-aren.com/vb/

by illustrations, of how to use the encrypted message program TELEGRAM.[13]

An image from the Shumukh al-Islam forum

Offensive Tactics

During April-June 2015, the discourse on forums included references to the attacks by groups and fighters affiliated with Al-Qaeda and the Islamic State. Posters commented on successful attacks, and uploaded videos threatening to wage an electronic war against the United States.

- A hackers group called Qaedat al-Jihad al-Electroniyya, which associates itself with Al-Qaeda, claimed responsibility for damaging a website belonging to the Lawyers Association in Vietnam.[14]
- A group of hackers called "The Electronic Caliphate", which identifies with the Islamic State, claimed responsibility at the beginning of April for hacking into the French Television network TV5Monde, and shutting down all of the channels for three hours. As part of the breach, threatening messages in three languages – Arabic, French, and English, were posted on the TV network's Facebook page. The messages called for the killing of the President of France, and stated that the electronic jihad intended to harm enemies of the Islamic State that collaborated with France and the United States in the war against the IS. Later, the group published a video in which the network's manager admits that the breach occurred.[15]

[13] https://shamikh1.info/vb/
[14] http://www.sunnti.com/vb/; http://www.shabakataljahad.net/vb/
[15] https://www.youtube.com/watch?v=iSKSnLYTkBI

An image from the breach of the TV5Monde network

- An anonymous jihadist media group called Uyan al-Umma published a video titled "The Electronic Caliphate Enters a New War". The video focused on the breach of a group of hackers – "The Electronic Caliphate" – into the French satellite channel TV5Monde.[16]

From left to right: the logo of the Uyan al-Umma media group; a segment of the video

- A group of hackers called the OmarXarmy Group, which identifies with the Islamic State, claimed responsibility for damaging a Shi'ite web site (http://www.alkadhum.org) and a Thai web site (www.rimphaka.ac.th).[17]

[16] https://twitter.com/als_HHH_mMmM/status/591090061946527744
[17] https://twitter.com/OlMuslimRadical/status/589135879303663616

- After Operation Decisive Storm (Asifat Al-Hazm) [Sunni countries lead by Saudi Arabia (including Egypt, Morocco, Jordan, and North Sudan) fighting against the Houthi rebels in Yemen (who received support from Iran)], Saudi Hackers initiated an electronic attack against websites belonging to Iran and also its supporters. For example, a Saudi Hacker claimed responsibility for hacking an Iranian server that supplied internet services in Iran: http://www.autcontrol.ir/.[18] Another Saudi hacker claimed responsibility for hacking into the YouTube and Twitter accounts of the Iranian satellite channel Al-Alam, in Arabic, on April 12, 2015. The hacker inserted a caption on the site, which claimed that Iran was conducting a false propaganda campaign against Saudi Arabia and the Gulf states, and which also vowed to wage war against anyone who tried to harm the Saudi Kingdom. Another hacker posted a video documenting a hack into the blog managed by Ansar Allah, the operational branch of the Houthis in Yemen.[19]
- A list of Iranian and Shi'ite websites that were hacked was uploaded to Twitter under the hashtags "Electronic Decisive Storm"[20] and "Breach of Websites and Accounts of the Safavids"[21] (An insulting name for Shi'ites, based on the Shi'ite Safavid Empire that ruled Iran in the 16th century).

Examples of corrupted hacked Shiite sites by "Electronic Decisive Storm"

Guidelines

- A blog in English called Ansar Kilafah, which supports the Islamic state, suggested using the

[18] #عاصفة_الحزم_الالكترونية
[19] https://www.youtube.com/watch?v=qwR9Q3QW4Qo
[20] #عاصفة_الحزم_الالكترونية
[21] #إختراق_المواقع_والحسابات_الصفوية

BitTorrent program to transfer files between computers.[22]

- The jihadist forum "The Technological People of The Caliphate State", which identifies with the Islamic State, published a series of lessons about hacking, in the "Hacking Practice" section. The series of lessons covered subjects such as: understanding Safe Mode, overcoming Safe Mode with a php.ini file, information mining via the login accessed with index.html or login.php, hacking into websites by inserting SQL, identifying weaknesses and security breaches in websites, and use of shell uploading as a tool for hacking into websites.[23]

The banner for the "Hacking Practice Course for Supporters of the Islamic State"

A clip from the video

Organizational Activities

The following section includes a report about the activities of groups and hackers who were active during this period. Activities of established groups affiliated with the Islamic State, such as IS Hacking Division, Cyber Caliphate, and ISIS Cyber Army are covered, alongside those of hacker

[22] https://ansarkhilafah.wordpress.com/2015/05/30/how-to-download-videos-from-the-website/
[23] http://www.s3cur1ty-is.com/vb/

groups that have recently started identifying with IS activity, such as groups from North Africa – mostly from Morocco. There is a noticeable increase in Muslim groups that changed their messages, and as part of the attacks that take the form of website vandalism, they have started exhibiting characteristics that indicate support for the Islamic State. In addition, there is an increase in significant cyber threats by groups affiliated with the Islamic State, made upon Western targets – mainly the United States.

There has also been an increase of attacks that damage websites, including messages supporting the Islamic State. However, it should be noted that most of the attacks were directed towards small sites with minimal security levels, and that no attack caused significant damage. Nevertheless, there were several significant attacks, such as the one on the French television channel, TV5 Monde. In addition, attempts to leak classified data by breaking into government sites has also been observed. It is estimated that in some of the cases, the documents publicized were already available to the public on the internet.

The Islamic State Affiliates

Cyber Caliphate

In early April, TV5Monde, a French television network, was forced to show only prerecorded material after Islamic State militants hacked into their server. "The Paris-based company, whose programs are broadcast in more than 200 countries worldwide, was the target of a cyber attack that is 'unprecedented for us and unprecedented in the history of television', TV5Monde manager Yves Bigot told AFP." In addition to taking over messaging on the website and preventing the network from broadcasting its material, the hackers also took over access to the network's social media sites and put out messages claiming to have information about resumes, and identity information about French soldiers fighting against the Islamic State. One message reading, "*Soldiers of France, stay away from the Islamic State! You have the chance to save your families, take advantage of it,*" was broadcast, as well as, "*The Cyber Caliphate continues its cyber jihad against the enemies of Islamic State.*"[24]

As far as what was being done to counter the attack, the French Foreign Minister said that the government and security forces were doing everything they could to restore normalcy and

[24] http://news.yahoo.com/french-tv5monde-hit-pro-islamic-state-hackers-222158856.html

prevent that kind of attack from happening again. France was in a complicated position as well, for not only were Paris and Paris suburbs subjected to two widely publicized terrorist attacks in January, but France is also part of the US-led military coalition to defeat the Islamic State, and 1,500 French nationals have left France to join ISIS as foreign fighters. This attack was seen as a much higher-level attack than previous cyber attacks

Following this cyber attack, the defense ministry in France claimed in April that the Islamic State hackers did not leak private government information when they hacked into the France network TVMonde.[25] Adding to their cyber-security issues, the French television station carelessly shared its YouTube password in a segment while reporting on the attack on air.[26] A new report indicated that hackers were able to infiltrate the TV system after getting journalists to respond to a Trojan malware, after a spear phishing attack back in January. This is changing the investigation into a focus on "human error."[27]

In an update published on June 10, a researcher from FireEye claimed that a Russian group known as AT28 might be behind the attack, using the Cyber Caliphate name to camouflage the its true identity, and that the attack was part of an experiment to test whether the group was able to interfere with the TV broadcast.[28]

Islamic State Hacking Division

- In early April, as a follow up precaution to the kill list that was released a few weeks ago, Marine Corps were being instructed to take extra safety precautions regarding social media use and putting their own names and information out online.[29] This appears to be a safety measure intended to keep the soldiers safer and more vigilant about their security. Additionally, unlike initial reports suggested, it did not appear that the names were collected through a hack of private systems within the Department of Defense, but actually from public sites.

[25] http://www.channelnewsasia.com/news/world/france-denies-tv5monde/1777516.html
[26] http://www.newvision.co.ug/news/666899-hacked-french-tv-station-admits-new-blunder-over-password.html
[27] http://www.thelocal.fr/20150414/how-the-french-channel-tv5-was-hacked
[28] http://www.buzzfeed.com/sheerafrenkel/experts-say-russians-may-have-posed-as-isis-to-hack-french-t#.kovZn1d7E
[29] http://www.marinecorpstimes.com/story/military/tech/2015/04/02/corps-to-marines-google-to-stay-safe-from-isis/70820358/

- In a video published on April 29, the Islamic State Hacking Division claimed to expose a member of the Anonymous hacker group. The video shows a CBS news interview with an Anonymous hacker who was arrested by police. The hacker claims that he was forced to work as an informant against other members of Anonymous. The video claims that the FBI was also involved in the collaboration with ISIS. The video claims that the FBI collaborator with the IS in exposing the hacker, and the video concludes with the music that the IS typically includes in their videos.[30]
- On May 13, an IS affiliated hacking group threatened an electronic war on American, European, and Australian sites. It claimed it had access to high level American intelligence and would perpetuate a major cyber attack that would cripple those regions of the world. The hack was carried out by "Islamic State's Defenders on the Internet" and the information was publicized through a video message entitled "Message to America".[31]

"Praise to Allah, today we extend on the land and in the internet," a hooded and anonymous figure with a masked voice says in Arabic in the video, accompanied by English subtitles. "We send this message to America and Europe. We are the hackers of the Islamic State and the electronic war has not yet begun. The electronic war has not yet begun."

"What you have seen is just a preface of the future. We are able until this moment to hack the website of the American leadership and the website of the Australian airport and many other websites."

The video banner

[30] http://sendvid.com/3j6lfa2l
[31] http://www.techworm.net/2015/05/isis-affiliated-hacking-group-threatens-a-all-out-electronic-war-against-usa-europe-and-australia.html

Screenshot from the video

- According to a news article released on May 17, the Islamic State video which threatened an electronic war on the United States was deemed by experts to be important enough to take seriously. Many experts believe that as the IS obtains more money, "they will be able to hire the talent they need or outsource to criminal organizations."[32] Experts also predicted an increase in the number of large scale attacks perpetrated by ISIS and its sympathizers over the course of the rest of this year.

Islamic State Cyber Army

- On March 24, the Islamic State Cyber Army released the following statement:

الحمد لله رب العالمين, والصلاة والسلام على سيدنا محمد الصادق الوعد الأمين.

Praise be to Allah, and peace and blessings be upon our master and guardian, the Prophet Muhammad, the Truthful, our Final Messenger

اللهم لا علم لنا إلا ما علمتنا إنك أنت العليم الحكيم,

Oh God, we have no knowledge except what You have taught us, the All Knowing, the Judge

إللهم علمنا ما ينفعنا وانفعنا بما علمتنا وزدنا علما

[32] http://thehill.com/policy/cybersecurity/242280-isis-preps-for-cyber-war

Oh God, who has taught us what benefits us, may You make what you have taught us useful, and may we become wiser

وأرنا الحق حقاً وارزقنا اتباعه,

And may You show us the Truth, and give us the ability to follow it.

وأرنا الباطل باطلاً وارزقنا اجتنابه

And may You show us the falsehood as false, and give us the ability to refrain from it.

واجعلنا ممن يستمعون القول فيتبعون أحسنه،

And may we be among those those who listen to Your Word and follow the best thereof

وأدخلنا برحمتك في عبادك الصالحين

Admit me by Your mercy into the company of Your righteous servants.

موقع ولله الحمد تم بحمد الله حصيلة اختراق 29

Thanks to Allah we have been able to hack into 29 sites

Your brother in God,
Hacker Caliphate State
@isis_cyberarmy [33]

Addressing Allah, the hackers claim that they defaced a number of Western websites with a defacement attack.

Islamic State Supporters

- On April 17, an Ithaca, New York real estate website was hacked. It appears that this attack was successful because once again, the website was insecure and built through WordPress. The motivations of the IS sympathizers who were believed to have hacked this site were unclear, but appeared to be 'ideological.'[34]

[33] https://justpaste.it/isis-cyberarmy2
[34] http://ithacavoice.com/2015/04/islamic-state-hackers-target-ithaca-real-estate-blog/

A hacked web page

While many of the hacks described above were initiated by specific groups known to carry out hacks on behalf of the Islamic State, for the most part the exact groups responsible were not publicized.

- On May 11, ISIS hackers threatened to carry out a cyber-attack that would "frighten America." At 9:00 AM Eastern Standard Time, Twitter suspended the account from which the attack was publicized. So far, no other information has been forthcoming.[35]

Screenshot from ISIS Caliphate twitter, warning of an attack.

[35] http://www.hngn.com/articles/91137/20150511/isis-hackers-announce-planned-attack-on-america-today.htm

Moroccan Islamic Union-Mail

The Moroccan Islamic Union-Mail, known also as MIUM, is a hacker from Morocco with over 1,500 known successful defacements.[36] It is not clear if MIUM is a person or a group, but it is considered to be pro-IS, and most of the attacks (about 1,300) to date have been mass defacements.[37] MIUM started to operate on February 2014. It is an anti-Israel, anti-Western collective and has targeted Jewish websites in the United States, as well as military websites in the United States and elsewhere in the Western world. The Moroccan Islamic Union has also hacked countries in the Middle East, claiming to: "defend Islam and fight injustice all over the world by defacing websites."[38] Some experts believe the MIUM group can be defined as an Islamic version of the cyber group Anonymous.

Screenshot of Moroccan Islamic Union

- On the week of April 7, the Moroccan Islamic Union hacked into the UK-Air website, the air-quality page of a British government's Department for Environment, Food & Rural Affairs

[36] http://zone-h.org/archive/notifier=Moroccan%20Islamic%20Union-Mail
[37] http://www.zone-h.org/archive/notifier=Moroccan%20Islamic%20Union-Mail
[38] http://www.middleeasteye.net/news/moroccan-hackers-take-over-saudi-government-website-pro-brotherhood-protest-1645652384

website.[39] The group defaced the website and replaced the forecasts for air pollution over the British Isles with a message criticizing Britain's involvement in Iraq invasion in 2003. The hacked website redirected viewers to the MIUM website, which displayed a picture of Saddam Hussein and the message: "I*t's time to remind the British government what you did with Saddam Hussein will not forget. And we are ready to sacrifice with everything, as not to give up Iraq and stay alert for the coming."*[40] Authorities are unsure of where the vulnerability in the website was that allowed the hackers access. [41]

- On May 24, the official website of the Nepalese Embassy in Washington was hacked by Moroccan Islamic Union. An anti-American message was left on the site concerning the invasion of Iraq and the subsequent war. The message read: "Iraq is the cemetery of American…hello to the death that awaits you at the hands of the mujahidin in Iraq." This was not the first time the website of the Nepalese Embassy had been hacked.42

MoroccanWolf

Moroccanwolf is a hacking group from Morocco with over 10,000 known defacements.[43] It is not clear if it is a person or a group. It is considered to be pro-IS as it uses IS content as part of its defacement attacks. Most of the attacks are mainly mass defacements.

- On April 17, the website of an Alabama nonprofit organization was hacked, displaying a message from the Moroccanwolf hacking group.[44] The owner of the site was shocked to learn of the hacking and the messages posted, but believes it was likely that many other small websites in the state were hacked - though perhaps they did not receive media attention. At that point, the website was taken down.
- Additionally, in early May, IS hacking affiliate Moroccanwolf hacked St. Vincent and the Grenadines website, posting Islamic State images, and anti-American and anti-NATO

[39] http://www.theguardian.com/technology/2015/apr/07/islamist-hackers-defra-air-quality-website-saddam-hussein
[40] http://rt.com/uk/247441-defra-jihad-hack-saddam/
[41] http://www.hotforsecurity.com/blog/uk-government-website-hijacked-by-islamist-hackers-11676.html
[42] https://www.hackread.com/nepali-embassy-usa-website-hacked/
[43] http://www.zone-h.org/archive/notifier=moroccanwolf/page=1
[44] http://wiat.com/2015/04/16/isis-sympathizers-linked-to-hacking-of-leeds-nonprofit-site/

messages.[45]

- In a separate incident, the Bahamas Tourism Website was hacked by Moroccanwolf – Islamic State.[46]

Moroccan Revolution

Moroccan Revolution Team is another hacktivist collective from Morocco, which started to operate in February, 2015. Based on its prior attacks, it is evident that Moroccan Revolution Team is likely a pro-IS, anti-Western group. Its main activity is website defacements with more than 600 successful attacks, of which about 400 were part of mass defacements.[47]

- On May 22, the Moroccan Revolution Team defaced the website of Westchester Health in the tri-state area. When patients navigated to the website for Westchester Health, they ended up on a webpage that declared the site had been hacked and read, "I love you ISIS," along with an image of the Islamic State's notorious black flag. The website was defaced for a total of 16 hours before being restored. No patient information was compromised.[48]

Phénoméne Dz

Phénoméne Dz is a pro-IS hacker located in Algeria, with DZ being part of the domain name for websites in Algeria. Phénoméne Dz targets Western countries allied with NATO, and has hacked websites in Egypt, Syria, Iran, Ukraine, Brazil, Serbia, United States, and Barbados. His main activity is website defacements.[49] He has successfully defaced over 1,600 websites, with over 1,200 as part of mass defacements.[50]

[45] http://indiatoday.intoday.in/story/isis-hacks-st-vincent-government-website-terrorism-iraq-islamic-state/1/433675.html
[46] http://www.tribune242.com/news/2015/may/14/national-security-fears-tourism-website-hacked/
[47] http://www.zone-h.org/archive/notifier=Moroccan%20Revolution
[48] http://pix11.com/2015/05/22/isis-hackers-take-over-local-healthcare-website-company-tries-to-assure-patients-their-info-is-safe/
[49] http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/phenomene-dz-a-pro-isis-pro-palestinian-hacker-from-algeria/
[50] http://www.zone-h.org/archive/notifier=Ph%C3%A9nom%C3%A9ne%20Dz

A sample of Phénoméne Dz's work

- On June 16, a website affiliated with the University of Baltimore was defaced with a pro-IS message. The Baltimore Neighborhood Indicators Alliance website was hacked by Phénoméne Dz. No sensitive information was compromised, but the following message was placed on the site: "Stay away from our land. You will pay today or tomorrow…#suicidebombersinUSA." [51]

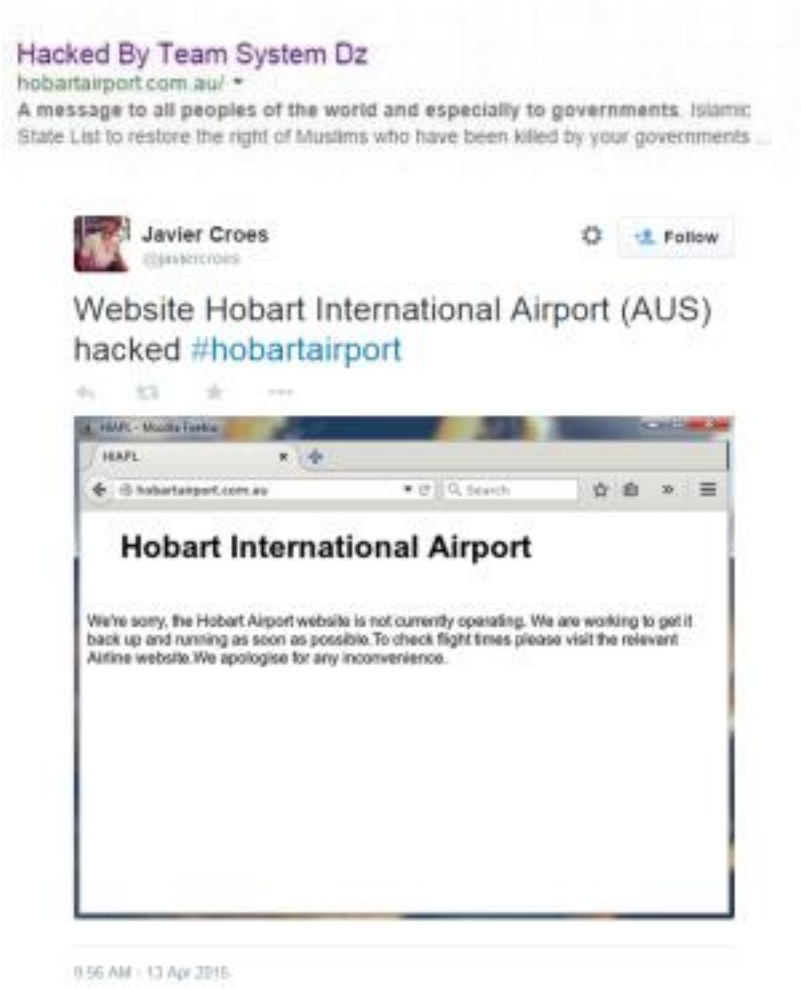
Team System DZ

Team System DZ is a pro-IS hacktivist collective that is also in support of a free Palestine. Team System DZ defaces over six websites a day. They hack insufficiently secured hosting providers, which allows them to breach a variety of websites. [52] The groups have successfully attacked over 7,300 websites, with more than 5,600 as part of mass defacements.[53]

- On April 12, Australia's Hobart Airport's website was down after a hack from the Islamic

[51] http://www.wbaltv.com/news/University-of-Baltimore-affiliated-website-hacked/33611654
[52] http://kevin.borgolte.me/notes/team-system-dz-isis-isil-defacement-campaign/
[53] http://www.zone-h.org/archive/notifier=Team%20System%20DZ

State.[54] Police had been monitoring the area on the ground at the airport as well, although specific threats had not been made to the airport or individuals in the area. Experts appeared to believe that this attack was part of an Islamic State strategy to "non-discriminately target organizations who use web hosts such as the one used by Hobart International Airport." [55]



Notification that the airport page was hacked

- The Wilmington Public Schools website was hacked by Team System DZ on April 23. The website was defaced and a message posted by the hacker read:

[54] http://www.theaustralian.com.au/news/nation/hobart-airport-website-shut-down-after-hack-by-islamic-state-supporters/story-e6frg6nf-1227300651102
[55] http://www.theaustralian.com.au/news/nation/hobart-airport-website-shut-down-after-hack-by-islamic-state-supporters/story-e6frg6nf-1227300651102

"Hacked by Team System DZ. I am Muslim & I love jihad. I love isis <3. A message to all peoples of the world and especially to governments. Islamic State List to restore the right of Muslims who have been killed by your governments savage and unjust Islamic state with restore dignity for Muslims Will purge the land of the Muslims from the hypocrites infields It intervenes you will equip you to dwell in cemeteries. Op USA & Israel." [56] [*this is the exact text as it appeared on the site – with several spelling and grammar mistakes*]

Abu Hussain Al-Britani

- On May 10 this Twitter account reopened after being shut down for some time, publishing posts[57] with new threats from the supporter of the Islamic State, against Britain and the West:

Screen shot of Abu Hussain Al-Britani's Twitter account

[56] http://patch.com/massachusetts/wilmington/developing-wilmington-schools-website-possibly-hacked-terrorist-group-0
[57] https://twitter.com/alamrikiya001/status/597441432333492224

The account featured a number of warnings[58], which included one post regarding "good news that will be heard soon":

Screen shot of Abu Hussain Al-Britani's Twitter account

RxR HaCker

RxR HaCker is a Saudi Arabian hacker of whom not much else is known. The hacker appears to be anti-Iranian, pro-Saudi and pro-Yemeni. RxR HaCker's attacks most often take the form of website defacements.

- On May 7, RxR HaCker defaced the official website of the Iranian Ministry of Defense and insulted Iran's leader Ali Khamenei over the war in Yemen. The defaced website read: *"Hacked by Rexer Hacker. I'm away most of the time and get respected by everyone…if I came back; I get loved as well as respected by all. Saudi Arabia will cut any finger that's pointed at Yemen. Yemen will remain (the origins of the Arabs) and its people will never accept filthy fire worshippers."* The specific page that was defaced was the recruitment department that details job placement of religious and ethnic minorities in the country's defense sector. [59]

The Middle East Cyber Army

The Middle East Cyber Army is an anti-Western and anti-Israel hacking collective that operates out of the Middle East. Not much is known about the characteristics of the collective, other than that it frequently defaces websites all over the world.

[58] https://twitter.com/AbuHu55ain_2
[59] https://www.hackread.com/saudi-hackers-iran-defense-ministry-website/

- On May 18, the Middle East Cyber Army defaced the website of the English Language Academy of the University of Auckland. When users searched for the university's website on Google, the link to the site read. *"Hacked by Middle East Cyber army. We are Muslims and we are proud!"* A second message in Arabic read, *"Lord God has chosen Islam as a religion and our master Muhammad as a prophet and a messenger."* The website was hacked for at least 12 hours, but no data was compromised. [60]
- The Middle East Cyber Army hacked into Arizona's State Department of Weights and Measures website, on June 10. No sensitive data was compromised and the director of the agency was not sure how the group got into the site. The site was covered with images of warfare, of raging flames, and a city coming down. There was also a message that said, "*In Allah we trust. For Allah we work*. *Death to Israel. Free Palestine. Jerusalem is ours*."[61]

H1d3n Root

Little to no information exists about the hacker who goes by the name H1d3n Root. He or she is responsible for a few instances of defacing starting from 2015.[62] The hacker is a member of Cyber Command0s (Team_CC)[63], a known groups with more than 8,000 defacements attacks, and likely from Bangladesh.

- The pro-Muslim hacker called H1d3n Root hacked the website for Philadelphia's City Council on May 20. The site was compromised for several hours and a black background with white text that read, "I am Muslim & Islam is my way of Life", replaced the usual page. Below that, it read "OpUSA" and "OpIsrael." No sensitive information was leaked or compromised during the hack and the City Council began working to upgrade security on its servers to prevent future attacks.[64]

[60] http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11450531
[61] http://www.azcentral.com/story/news/arizona/politics/2015/06/10/arizona-agency-website-hacked/71007982/
[62] http://www.zone-h.org/archive/notifier=H1d3n%20Root
[63] http://zone-h.org/archive/notifier=Team_CC?zh=1
[64] http://www.philly.com/philly/blogs/heardinthehall/City-Council-website-hacked.html

Screen shot of Cyber Command0s Twitter account

The Yemen Cyber Army

The Yemen Cyber Army (YCA) is a hacktivist collective likely based in Yemen. There have been indications that the Yemen Cyber Army is backed by the Iranian government and may even operate partially from Iran. Yemen Cyber Army's activities include website defacements and even more sinister deployment of malware in Israel, Saudi Arabia, and Yemen, likely used for state espionage.[65]

- On May 22, Yemen Cyber Army defaced the Saudi Arabian Ministry of Foreign Affairs website and leaked the login credentials of Saudi officials, conversations between embassies, and embassy VSAT communications. This was followed several days later with the release of records of the Saudi VISA database and a threat to release more. The hacktivist collective said the reason for targeting the Saudi ministry was to convey a message to the government against its attack on Yemen.

[65] http://www.buzzfeed.com/sheerafrenkel/who-is-the-yemen-cyber-army#.fgyWgEA9P9

Allah is the enemy of those who oppress people

This is to convey a message to Saudi Dictators, if they've got a listening ear!

It's us again, Yemen Cyber Army!

We are an Islamic Group who fights against you oppressors.

What you and your puppets commit in Yemen, Syria, Bahrain, Iraq and Lebanon, remind us of crimes your forefather Yazid-ibn-Muawiya committed in Karbala. And indeed you are good successors to him. You are ISIS and ISIS is you.

Never assume our calmness is due to weakness. We are oppressed! God will judge between you and us. As we never seek help from other than him.
You are pagan oppressors as you always fawn for US and Israel, that's what you deserve.
So congratulations to those who achieve martyrdom in fight against pagan oppressors.

"And never think of those who have been killed in the cause of Allah as dead. Rather, they are alive with their Lord, receiving provision "

Our cyber operation is just started and by the grace of God we are expecting the Saudi regime's collapse by the "Labbaik Ya-Hossain" slogan.
This second operation is blessed by the name of martyred "Syed Hussein Badreddin al-Houthi" and is going to be a beginning to Saudi's overthrow, Inshallah.

We have gained access to the Saudi Ministry of Foreign Affairs (MOFA) network and have full control over more than 3000 computers and servers, and thousands of users. We also have access to the emails, personal and secret information of hundreds of thousands of their diplomats in different missions around the world.

We publish only few portions of vital information we have, just to let them know that "truly the flimsiest of houses is the spider´s house"

Some portions of visa secret information, thousands of documents from the MOFA's automation system and secret emails will be published gradually so as to keep Saudi puppets always in fear of their identity disclosure.

This way they might slightly come to know how it feels when our innocent women and children rush into havens crying and looking for their beloved once in dark.

And that's not all! All your computers will be automatically wiped on Wednesday - 2015 20 May and at 12:00 to become a lesson for oppressors.

We have the same access to the Interior Ministry (MOI) and Defense Ministry (MOD) of which the details will be published in near future. Wish such shocking news make Saudi dictators to come to their senses and recapture those young wild dogs' leash to avoid Muslims exploiting hate against Saudi family.
If you did not stop attacks on Muslims in Yemen, do not blame anyone but yourself and expect greater harms.

The message with links to the leaked files[66]

This attack was the largest cybercrime orchestrated by the YCA against the Saudi government. The group has claimed it has access and full control over more than 3000 computers and servers, as well as classified files and correspondence of senior Saudi officials with other countries

[66] http://pastebin.com/w1iVBMiE, http://pastebin.com/MdHUEMeJ ,http://pastebin.com/kPtiGcEf

Izzah Hackers

Izzah Hackers is a non-geospecific Muslim collective. They describe themselves as "hacktivists for justice against oppression and hatred worldwide." They are anti-Israel, pro-Palestinian and are heavily involved in #OpIsrael. Its activities include website defacements and attainment, and dumping of personal accounts of Israeli government officials. [67]

- On April 18, Izzah Hackers posted[68] information about a leak from the Jewish Press website. The link contained 18 TXT files that displayed information about users and statistics allegedly from the website.

The Izzah Hackers Tweet

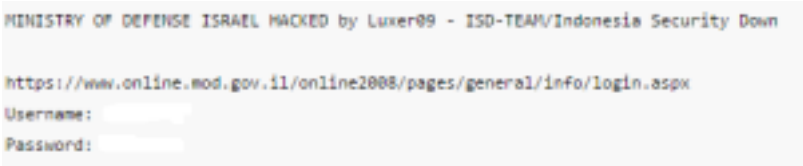
- On June 4, Izzah Hackers hacked the French telecom company Orange and leaked the details of 4,597 customers. The hack took the form of a phishing attack and was documented by police. Izzah Hackers is a pro-Palestinian Muslim group. [69]

[67] http://thecryptosphere.com/2015/04/09/exclusive-interview-with-opisrael-hackers/
[68] https://twitter.com/IzzahHackers/status/589489542157230080
[69] http://blog.sensecy.com/tag/izzah-hackers/

Luxer09

Luxer09 is an Indonesian Hacker, part of ISD-TEAM. The hacker has been active since April 2013, with over 200 defacements as part of mass defacement attacks.[70] His targets are mainly Western, and he claims the ownership of the websites he hacks

- On June 1, the hacker published a statement in which he claimed to possess the access details (name and password) of the electronic trade site of the Israeli Ministry of Defense.[71] The post was signed "Luxer009-ISD-TEAM/Indonesia".



The Luxer09 June 1 post

The Syrian Electronic Army

- On March 21, the Syrian Electronic Army published an announcement on behalf of the SEA Programming Unit about the improvements made to the Syrian Electronic Army website. Improvements have made from time to time on the organization's site, including a number of total changes to the user interface.
    - The first improvement[72] was the launch of a new version of the site:

[70] http://www.zone-h.org/archive/notifier=luxer09
[71] http://pastebin.com/s97vZYEe
[72] https://twitter.com/SEAPU_Official/status/582649134726823936

- The second improvement was an update that enabled higher quality viewing from cellular phones.[73]

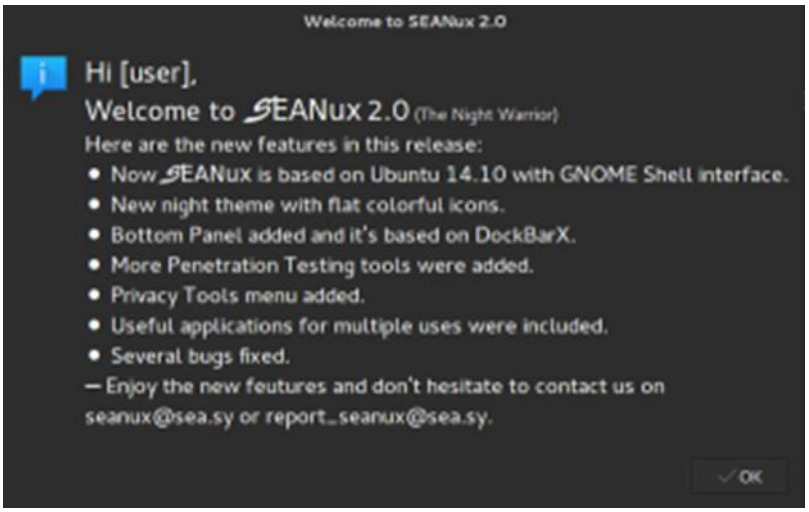
A screenshot from the page about improved cell phone viewing

[73] https://twitter.com/SEAPU_Official/status/582652241040936960

- On April 10 the Programming Unit of the Syrian Electronic Army published a statement[74] about the upcoming release of SEANux 2.0 "The Night Warrior" – an operating system based on the Linux supported Ubuntu system, which is an open source allowing programmers to make adaptions according to their personal needs. The system includes hacking tools, and protection of the user's anonymity. The system was scheduled to be released on May 1. (The first version of the program SEANux1.0 was launched[75] on November 1, 2014, and on February 8 it was announced that version 2.0 would soon be available, with a description of the version also posted.)

The announcement about the new release

[74] https://twitter.com/SEAPU_Official/status/586279145518272513
[75] https://twitter.com/SEANux_Official/status/528619046753689601



Features of SEANux2.0

- On April 22 the Syrian Electronic Army posted on its Twitter account[76] a general warning to the enemies of Syria, stating, "A hand that will target Syria will be cut off". A photograph of Bashar Jaafari, the Syrian ambassador to the UN, appeared in the post.

The threatening April 22 post

[76] https://twitter.com/Official_SEA16/status/590976588780535808

- On April 23 it was publicized[77] that as a result of an information leak incident in which a woman he was having an affair with was given information, General David Petraeus - a former commander of the multi-national forces in Iraq and Afghanistatan and former C.I.A. director – received a suspended sentence of two years and a fine of $100,000 dollars. That was as a result of an FBI investigation that began at the end of 2012. The day after the sentencing, the Syrian Electronic Army published two posts stating that it was possible it had access to the general's email account around July, 2013.
    - The first post[78] included a purported screen shot of logging in to the gmail account:

[77] http://www.nytimes.com/2015/04/24/us/david-petraeus-to-be-sentenced-in-leak-investigation.html?_r=0
[78] https://twitter.com/Official_SEA16/status/591598892690604032

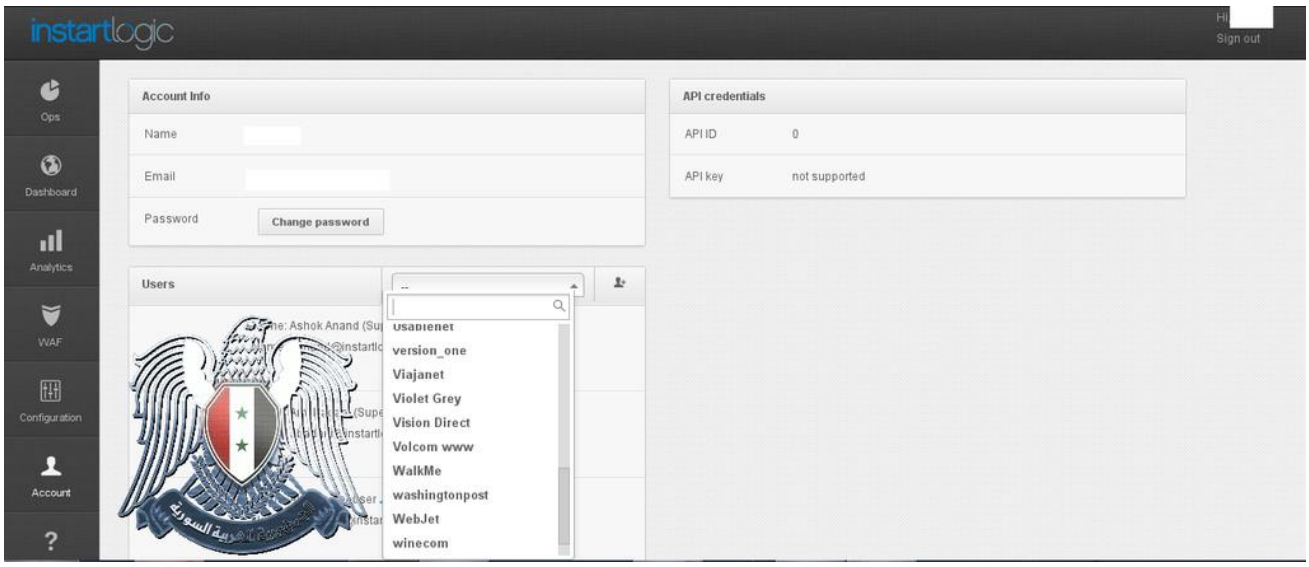
- The second post, included a supposed page from the general's US military email account ,[79] was published twenty minutes later:

In response to the post, which raises doubts about the truth of the hack, others who claimed to have performed that hack long ago posted evidence[80] that the SEA claim was fabricated:

[79] https://twitter.com/Official_SEA16/status/591603827742224384
[80] https://twitter.com/Official_SEA16/status/591601137553383424

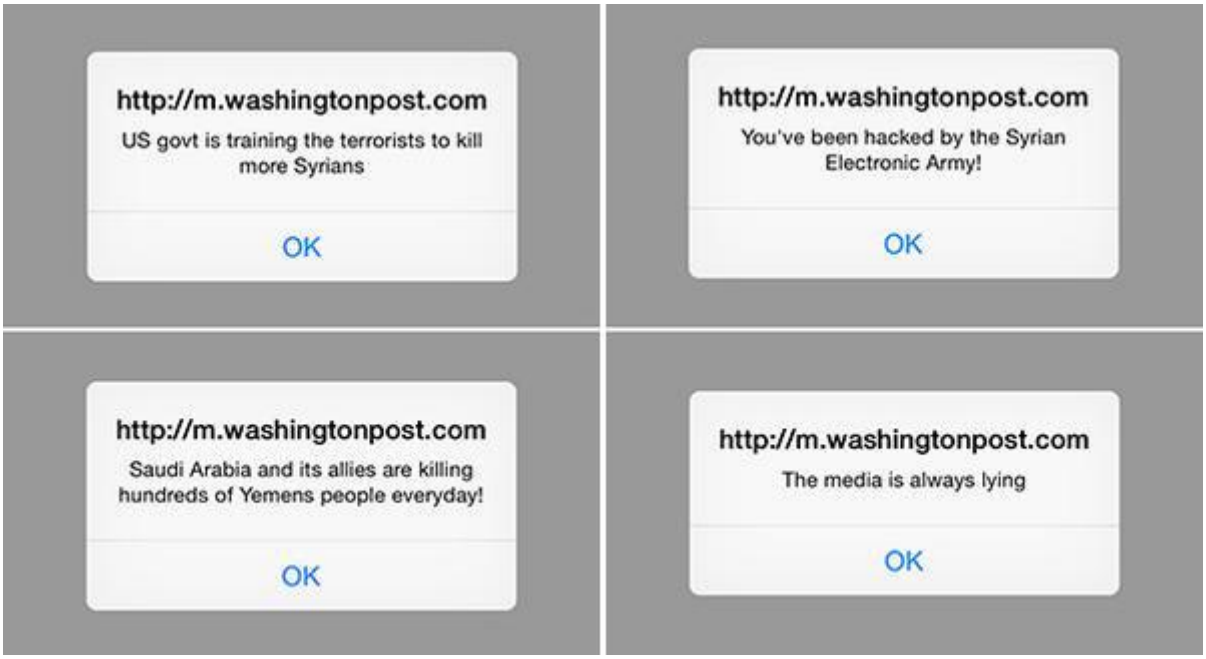
- On May 14, a post on the SEA Twitter account[81] stated that it had hacked the cellular site of the Washington Post:

The post included two images. One was supposedly from the newspaper management:



And the second displayed four notifications that were supposedly sent by the organization as part of the hack:

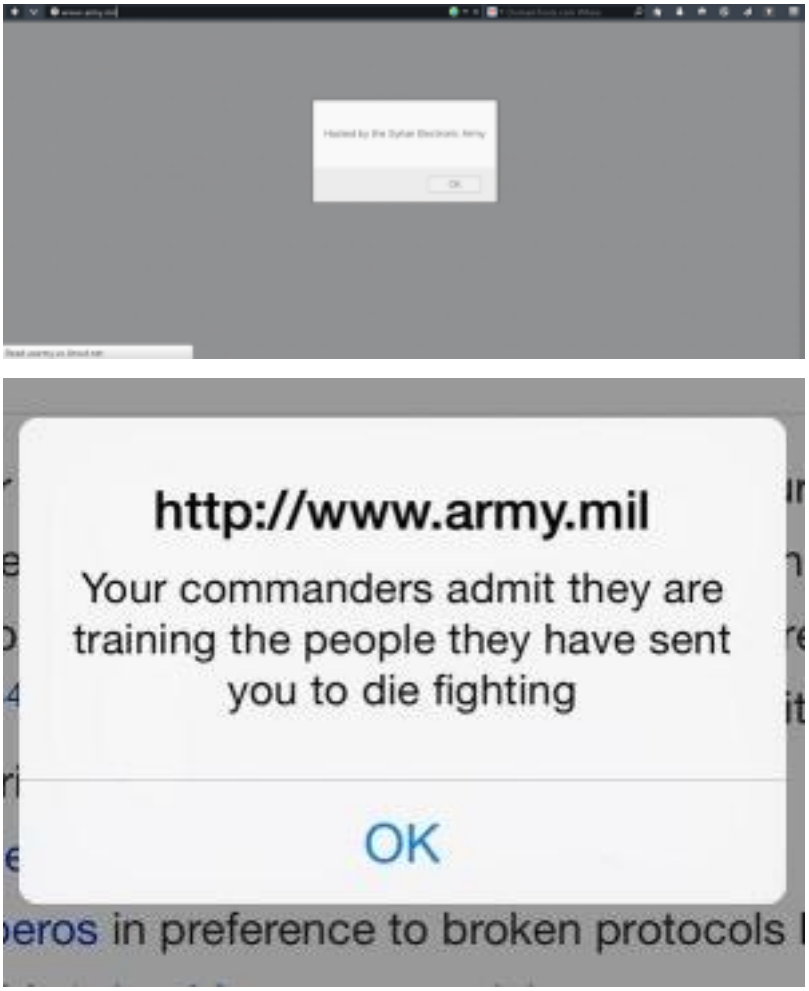
[81] https://twitter.com/Official_SEA16/status/598915099328282624



- On the evening of June 8, the Syria Electronic Army published on its Twitter account[82] and on its internet site[83] announcements stating that it had succeeded in hacking and defacing the United States Army site,[84] after discovering a weakness that had made it possible to take control[85] of the content administration section of the site.

The hack made it possible for the SEA to place a few announcements on the site,[86] including a call for the United States to stop training "terrorists" in Turkey and in Jordan:

[82] https://twitter.com/Official_SEA16/status/607952411366465536
[83] http://sea.sy/article/id/2083/en
[84] http://www.army.mil/
[85] https://twitter.com/Official_SEA16/status/607957210241617920/photo/1
[86] https://twitter.com/Official_SEA16/status/607974042679832576



It was also claimed that during this and other hacks, the organization was able to access information that would be published later, as the need arose.

Dr. SHA6H

Dr. SHA6H is a Syrian hacker whose focus is on issues within Syria. He or she is an anti-Assad hacker whose activities mostly constitute defacements, and who targets governments that are pro-Assad, as well as Western nations like the United States, and by proxy, Israel.

On May 24, Dr. SHA6H hacked the Uzbekistan Embassy site in Kuwait, and demanded that governments around the world bring peace to Syria. A message on the website read:

> *"This site has been hacked because of the world's silence about the (four) years of massacres that occur in Syria and that are still happening. This security breach is not to cause damage; it is only to deliver a specific message to the world. For three years the Syrian people have been suffering from hunger, thirst, and cold, and lack of attire, there are women raped, and children are dying, and*

houses have been destroyed, and kids do not know their destiny, and after all that the world accuses us of terrorism. We are not here to defend ourselves, but we came here to show you the truth. The USA made Osama bin Laden, and helped him and provided him with money and weapons, then called him a terrorist. Then got rid of him when it wanted to. The USA now supports Bashar al-Assad, the president of the Syrian massacre, but soon will call him a terrorist, as happened with Osama bin Laden, and then will get rid of him too. But do you know why the US doesn't want to get rid him now? She allows him the opportunity to kill the largest possible number of Syrian people. Do you know why? To make the task easier for Israel. This is the truth, you are judge…"

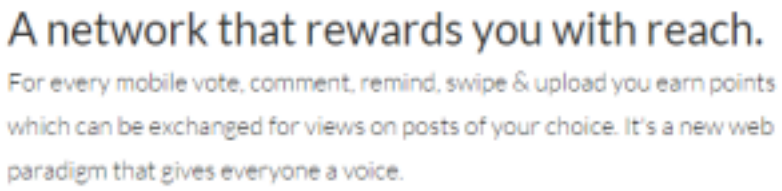
Dr. SHA6H has been known to hack government websites in the past.[87]

Anonymous

- On May 5, Anonymous published[88] an announcement claiming that seven email addresses and access passwords from the Baltimore Police were leaked, as part of an online campaign called OpBaltimore after the death of Freddie Gray – a young man from Baltimore who was killed the police during his arrest. After the file was published,[89] it was claimed that all of the contact and access details[90] to the Baltimore Police Department website were tested, and not one of them enabled entry into the system. But it is not clear if that is because the data was not exact, or because the passwords were changed. However, out of the seven email addresses, six belonged to active members of the Police Force, and one belonged to someone who was no longer in the Force. The information acquired is of the type that can be found online without difficulty, which suggests that there was no leak at all, but simply that someone gathered available information from different sources, including social media sites. It was also claimed that a similar list[91] had been posted in the past, alongside reports of a hacking attack intended to stop service[92] on the police site on April 28, but which in fact had little impact on the site's availability.

[87] https://www.hackread.com/anti-assad-hacker-hacks-uzbek-embassy/
[88] http://www.ibtimes.co.uk/anonymous-publishes-baltimore-police-officials-emails-passwords-after-freddie-gray-death-1499742
[89] http://pastebin.com/HtJRNTPM
[90] http://www.baltimorepolice.org/user/login
[91] http://pastebin.com/WdVpyAFf
[92] http://www.scmagazineuk.com/baltimore-city-government-website-knocked-offline/article/412227/

- On May 18, "Anonymous Italy" published[93] an announcement about a hack carried out, according to their claim, into the Italian Ministry of Defence computer system. The announcement included[94] a link to a compressed file that contained 42 CSV files, and directed views to an online LSX file[95] containing 1,748 entries, which included names, email addresses, positions, and company.
- On June 17, Anonymous announced[96] the existence of a new social media site supported by Anonymous, and guaranteeing privacy, security, and transparency when promoting posts. These types of platforms, with high standards of anonymity and security, make no distinctions between users. Therefore, they may become communication tools for crime and terror elements who then become a challenge for law enforcement officials. The network Minds.com,[97] which can be downloaded as an application, includes the basic features offered by any other social network, such as sending updates to followers, displaying comments, and advancing posts already read. But it is different from other networks in that it had no intention of earning money or collecting information. Instead, it encrypts all of the messages so that the advertisers or the government cannot read them.



A screenshot from the application

Therefore, it is claimed that the algorithms on this network are simpler than those on Facebook. The site is based on an open source that can be viewed on the Minds.org site,[98] though at present only the application source[99] is available. However, it is possible to join[100] the community of developers.

[93] http://anon-news.blogspot.it/2015/05/ministero-difesa-hacked.html
[94] http://wikisend.com/download/595518/Difesa_CSV.rar
[95] https://docs.zoho.com/sheet/ropen.do?rid=uboup5abbafd1f4574f658937a363a8d6834c
[96] http://rt.com/news/267835-social-network-anonymous-minds/
[97] https://www.minds.com/
[98] https://www.minds.org/#/
[99] https://github.com/Minds/mobile
[100] https://www.minds.com/groups/members/100000000000000681

Meanwhile, more is hidden than revealed, but the site had about 60 million hits before it was even officially launched on June 15. However, many of its pages are empty of any content, including the pages "Terms",[101] "Privacy", and even the "About" page. [102] It also turns out that there is an initiative on the part of Anonymous to support this media network, as proven by a permanent ad on the Facebook page "Anonymous Art of Revolution".[103]

- On June 17 it was published[104] that elements that identified with Anonymous shut down the Canadian Government websites for several hours, probably in the form of a "denial of service" attack[105]. The hack was in protest of a controversial law passed to prevent terror – law 51-C, which "significantly broadens the authority of the intelligence agency in the country." This was in response to the first terror incident that occurred in Canada, in October 2014. Various government representatives[106] authorized the incident, but at the same time claimed that no personal data was stolen during the hack.

One of the posts about the attack provides the addresses of four Canadian government sites:[107]

[101] https://www.minds.com/p/terms
[102] https://www.minds.com/p/about
[103] https://www.facebook.com/pages/Anonymous-ART-of-Revolution/362231420471759
[104] http://nr.news-republic.com/Web/ArticleWeb.aspx?regionid=3&articleid=43499189
[105] http://globalnews.ca/news/2060036/government-of-canada-servers-suffer-cyber-attack/
[106] https://twitter.com/TonyclementCPC/status/611231622843789312
[107] https://twitter.com/OpCyberPrivacy/status/611225540188602368

Five days earlier, a video was posted called "Anonymous – Warning All Canadian Citizens in 2015",[108] in which there was a long statement against the law and its effects on personal freedom: https://www.youtube.com/watch?v=krmCViA9oKY.

El Moujahidin

El Moujahidin is a hacking group from Algeria. It is an anti-IS[109] and pro-Palestine hacktivist group. Its main activities are defacements.

- On April 10, the Turkmenistan Embassy Website in Belarus was hacked by a group claiming to be "Islamic State Hackers (El Moujahidin)."[110] The group posted a photograph of a man wearing a black mask with the IS logo, holding an AK-47. The following messages accompanied the photograph: "Hacked by Abdellah Elmaghribi…the website is in the service of the regime…#Struck by Abdellah Elmaghribi and Moroccan Wolf. By ISLAMIC STATE HACKERS (El Moujahidine) Your Security Get Owned." Because the country of Turkmenistan has been

[108] https://www.youtube.com/watch?v=krmCViA9oKY
[109] https://twitter.com/ElMoujahidin/status/600625693186248704
[110] http://thediplomat.com/2015/04/turkmenistan-embassy-website-hacked/

consistently neutral throughout its history, this appears to be an attempt to force the country to take sides in the war against (or with) the Islamic State. Earlier this year, Turkmenistan asked the United States for help in dealing with the Islamic State threat at their southern border with Afghanistan. Although it has yet to be confirmed that IS was actually behind this cyber attack, this feeds into the country's fear of threats.

- The Old Dominion University student newspaper in Norlfolk, Virginia was hacked by a group claiming connections to Algerian terrorists and referring to themselves as "El Moujahidin." (Islamic Hackers). A recent FBI statement related to the frequency of these attacks stated that "these types of incidents, whether disruptive or merely distracting, highlight the prolific nature of cybercrime."[111]

ODU's Student Newspaper website

[111] http://hamptonroads.com/2015/05/old-dominion-student-newspaper-website-hacked

Cyber of Emotion

Cyber of Emotion is a Saudi hacker group that began operating in 2014.

- On April 12, the group publicized[112] that the English Twitter account of the Iranian AlAlam News[113] channel had been defaced, and false announcements were posted Iran causing the death of the rebel leader in Yemen. At the same time reports were released about a hack into the station's YouTube channel, posting a song on the channel that praised the King of Saudi Arabia, with the Kingdom's flag in the background. News of and a claim of responsibility for that hack[114] was published on the Cyber of Emotion's Twitter account:

A description of the hack was also published

[112] http://www.zawya.com/story/Irans_state_TV_social_media_accounts_hacked-TR20150412nL5N0X9027X2/
[113] https://twitter.com/alalam_news
[114] https://twitter.com/Cyber__Emotion/status/587086348726755328

Confirmation of the hack was broadcast by another Iranian television channel, Sahar TV.[115] It seems that at the same time,[116] the group was also able to break into the organizational emails of the Iranian station:

[115] http://english.sahartv.ir/news/8780?utm_medium=twitter&utm_source=twitterfeed
[116] https://twitter.com/Cyber__Emotion/status/587847071144796161

And then the list[117] containing many details about the channel's employees was leaked:

TunisianHackers Team

On May 5, an announcement was published (in English[118] and in Arabic[119]) on the Tunisian Hackers Team Twitter account, saying that Tunisian police had arrested the leader of the group the day before. He was accused of involvement in hacking into American government sites as part of the #TheWeekOfHorror campaign.[120]

[117] https://twitter.com/Cyber__Emotion/status/587858971370860544
[118] https://twitter.com/XhckerTN/status/595682552419069952
[119] https://twitter.com/XhckerTN/status/595682911820611586
[120] https://twitter.com/hashtag/TheWeekOfHorror?src=hash

Hamas

On May 15 Yom HaNakba is celebrated, and in preparation for marking this date, Hamas announced on May 14 in its Twitter accounts in English[121] and in Arabic[122], that special hashtags would be used to refer to the date, including one in Hebrew in use from that date:

The post from May 14 with a hastag in Hebrew

In addition, different announcements were published, with some including subtitles in Hebrew and intended directly for the Israeli public:

[121] https://twitter.com/qassamsms/status/598786764585730048
[122] https://twitter.com/qassam_arabic1/status/598785250018242560


عائدون إلى كل مدينة وقرية ومزرعة أخرجنا منها عنوة مهما طال الزمن
חוזרים לכל עיר כפר וחווה שגורשנו מהן בעל כורחנו בהקדם או במאוחר


إذا كنتم تحتفلون بالاستقلال على بحر من دمائنا
فتذكروا أن كل الطغاة فعلوا ذات الشيء ولقد زالوا من الوجود
אם אתם חוגגים את העצמאות על ים דמנו
אז זכרו שכל העריצים עשו אותו דבר ועכשיו הם אינם

Al-Qassam Electronic Brigade

- كتائب القسام الإلكترونية[123] opened a Facebook Event called #Op_Free_Aqussa,[124] calling for an online attack against Israel on May 29, 2015.
- On May 30 the organization published[125] an announcement claiming it had leaked the details of 200 Israeli Facebook accounts. The announcement included a link to a file containing 252 email addresses and passwords.[126] Despite the fact that the file professed to contain details from Israeli Facebook accounts, 124 of the addresses ended with DE (Germany), 24 ended with CH (Switzerland),and 5 ended with FR (France), while not even one ended with IL or had any other signs of belonging to Israeli users. Therefore, it would seem that there the list is not credible, at lease with regard to the claim that it includes the details of Israeli Facebook users.

Gaza Hacker Team

Gaza Hacker Team is an anti-Israel, pro-Palestinian collective that hacks Israeli websites and pro-Israeli websites abroad. Its main activities include defacements and the use of malware via phishing attacks.

- On April 14, Mr.Le0n & Claw & Casper (part of the Gaza Hacker Team) hacked the website of The Jewish Press. It defaced the homepage of the site with a black backdrop and a man on horseback holding an IS-type flag. There was also a message in Arabic translated as: “Death to your entity mutant named ‘Israel.” Experts claimed the Jewish community would be vulnerable to such attacks in the future, and that such attacks should not be underestimated.[127]

[123] https://www.facebook.com/Al.Qassam.Brigades.1
[124] https://www.facebook.com/events/1669106479978235/permalink/1676364472585769/
[125] https://www.facebook.com/Al.Qassam.Brigades.1/posts/843569435735103
[126] http://pastebin.com/DLt77T2H
[127] https://www.hackread.com/pro-israeli-jewish-press-website-hacked/

The image posted on the Jewish Press site by hackers

AnonGhost

- On April 4, the hacker group AnonGhost published[128] an announcement on its Facebook account, claiming that they donated money stolen from Israelis by stealing their credit card details:

128

https://www.facebook.com/Anonghost.Team.Legend/photos/a.1524342334492578.1073741828.1524217164505095/1579819452278199/?type=1

A screenshot from the Facebook page

Cyber-Crime and Cyber-Terrorism, April – June 2015

Recent years have seen an increasing number of cyber-attacks against political targets, critical infrastructure, and the websites 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 from April – June 2015.

[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.

Attacks on the Operating System of the Polish Airline

On June the Polish Airlines LOT published an official statement[130] on its internet site, stating that it was sorry to announce that due to "a failure of the IT systems", the company was forced to cancel 20 flights.

In another statement[131] on the same day, the airline reported an "IT attack" that had affected the ground operating systems – something that made it impossible to prepare flight plans, and lead to the cancellation of outgoing flights from Warsaw. The announcement emphasized that the flight systems had not been affected, and that planes already in the air would continue their flights and return to Warsaw as scheduled.

The third statement[132] on that date said that everything was under control after the attack. The company was working to return its system to normal working order as quickly as possible. The operating system was working to prepare new flight plans, and was updating the passengers about the status of their flights.

Attacks on Government Sites

- On May 11, the Kenyan President's internet site[133] was hacked[134] by an Indonesian hacking group called "Gantengers Crew". The incident was documented.[135]
- On May 15, a Cyber attack[136] against the Bundestag site in Germany was announced[137]. Sensitive information was leaked. According to the announcement, which relied on an article on the subject that was published that afternoon on the Spiegel German news site,[138] the German Parliament was the victim of a Cyber attack during which unknown perpetrators hacked into the internal communication information network. According to the report, the Bundestag spokesperson authorized that the attack had damaged highly sensitive data, and emphasized

130 http://corporate.lot.com/pl/en/press-news?article=772898
131 http://corporate.lot.com/pl/en/press-news?article=772922
132 http://corporate.lot.com/pl/en/press-news?article=772947
133 http://www.president.go.ke/
134 https://www.hackread.com/kenya-president-website-hacked-indonesia-crew/
135 http://zone-h.com/mirror/id/24287890?zh=1
136 http://cyberwarzone.com/cyber-attack-on-bundestag-highly-sensitive-information-breach/
137 http://bundestag.de/
138 http://www.spiegel.de/netzwelt/netzpolitik/cyber-angriff-auf-den-deutschen-bundestag-a-1033984.html

that German security experts, together with the country's Intelligence authorities, were at that time investigating the attack. For security reasons, parts of the system were temporarily shut down, including the investigation committee's communication system, which was investigating the BND and NSA spying affairs.

At the same time, it was reported that the Bundestag site was apparently the victim of a "denial of service" attack.[139] The announcement referred to a Facebook account under the name "Captain Carlo"[140] (who claims to manage a Facebook page called "Anarchy Squad"[141], which like the Twitter page[142] opened on the day of the attack) – a figure who claimed responsibility[143] for shutting down the site and published a screen shot of the allegedly disabled site as proof.

A screenshot from the disabled site

Later, a link to a 25 second long video[144] was posted on the account, which professed to prove the site had been disabled. However, it may very well be that Bundestag itself initiated the temporary shutdown, as part of the security system check to determine if indeed a breach of the internal systems of the site had occurred. In any case, the site was soon back to normal functioning.

- On June 2, a Vietnamese news site published[145] that over 1000 local sites, mostly government and educational in nature, were hacked and defaced during the last weekend of May. That was

---

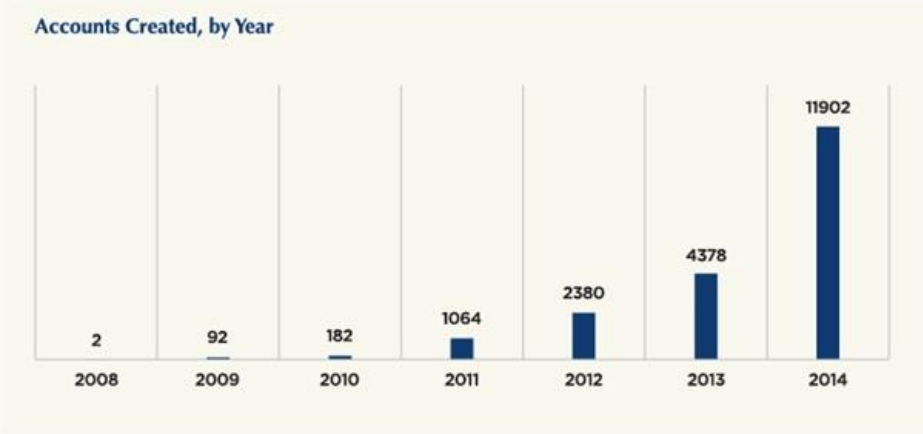
[139] http://cyberwarzone.com/bundestag-under-dos-attacked/
[140] https://www.facebook.com/official.captain.carlo
[141] https://www.facebook.com/AnarchySquad.Gods
[142] https://twitter.com/AnarchySquadGod
[143] https://www.facebook.com/official.captain.carlo/photos/a.1618371138374748.1073741828.161835820504 2708/1630343477177514/
[144] https://www.youtube.com/watch?v=sVcWQRqzpYw
[145] http://www.thanhniennews.com/tech/over-1000-vietnamese-websites-hacked-by-chinese-during-weekend-report-45148.html

in addition to over 200 sites that were hacked in the Philippines. The hack occurred during the Shangri-La Dialogue 2015 regional convention held in Singapore, in order to discuss the problems that arise because of conflicts between China and other South-eastern Asian countries. The hackers uploaded to the sites messages related to the conflict between China and Vietnam regarding southern China and the East Sea.

OpISIS

A study published[146] in March 2015 in the United States examined the activities of Islamic State supporters on Twitter. The study found that between September and December 2012 there were at least 46,000 Twitter accounts – though not all were active – belonging to supporters of the organization. However, that figure is a very conservative estimation, and according to the authors of the study, the maximum number of accounts may be as high as 70,000. At least one thousand of the accounts were deleted by Twitter during that period, and probably another two thousand later on.

The accounts with the most activity and biggest number of followers were those with the greatest risk of being deleted. The act of deleting accounts has a great influence on limiting the impact the Islamic State can make on the social media networks, even if the activity is not completely wiped out. However, accounts that are removed create new dangers, such as an increase in the rate of radicalization of the organization's fans on the media networks.



A graph showing estimated numbers of Twitter accounts of IS supporters. Brookings Project.

[146] http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf

The organization's typical supporters came from Syrian and Iraq. In addition, hundreds of accounts of IS supporters were published in tweets that stated their locations in combat areas.

Three quarters of the account users selected Arabic as their primary language for using Twitter, while almost one out of five chose English. An average IS supportive account had about one thousand followers, which is significantly higher the number of followers of accounts not related to the politics or war. In addition, the accounts of IS supporters were significantly more active than the accounts of regular users. It is estimated that most of the organization's online activity was mostly the work of a small group of between 500 and 2,000 accounts, defined as "hyperactive users".

In this context, it should be noted that users who identify with Anonymous have been extremely active for the past year against the Islamic State and the countries that support it. The emphasis has been on monitoring Twitter accounts of elements that identify with the organization, alongside publication of the guidelines for finding such accounts, keeping tabs on them, and reporting to Twitter accounts that should be deleted. In this framework, on April 10[147] a statement was published providing guidelines formulated by elements who identified with the OpISIS operation, with regard to steps that anyone who desires can take to contribute to the operation, as well as exposure of such accounts:

"#GhostSec #OpISIS

Contributing to Operation ISIS

Many individuals worldwide have shown an amazing amount of support in regards to Operation ISIS and have asked how they can contribute to our cause. The steps below can be used to track Islamic State Twitter accounts and their websites.

-1-Locating an Islamic State Twitter account.

If you are new to this locating an Islamic State Twitter account can prove to be difficult however after locating your first account you will be able to find thousands more following these steps. ISIS Twitter users are being aggressively hunted by Ghost Security and are called out for suspension on a regular basis. To locate an ISIS account Twitter search the hash tags #GhostSec or #OpISIS and you will find your first Islamic State Twitter account.

-2-I have located my first Islamic State Twitter account.

Now that you have located your first Islamic State Twitter account you will be able to collect many more and form a vast network of information. With the account you initially located review all of

[147] http://pastebin.com/UWWyaPRX

their following and followers collecting Twitter account names as you move forward. When you are collecting account names you must retrieve their Twitter ID by visiting the following website http://gettwitterid.com If you do not collect the account ID they can easily change their account name to evade you as they commonly do once detected. As you are collecting ISIS Twitter accounts check each bio and their tweets for website URLS and collect the information. With the data you have compiled visit http://pastebin.com and publish a paste of your findings and remember to save the Pastebin link.

-3-I have a Pastebin link of Islamic State Twitter accounts and URLS.

Now that you have collected this information you can take action against them by reporting your findings to Ghost Security. If your Pastebin link contains Islamic State Twitter accounts you can tweet your link making sure to use the hash tag #CtrlSec so their operatives can collect your information and terminate the accounts. If you have located Islamic State website URLS visit http://ghostsec.org and submit your Pastebin link so their operatives can collect your information and disable the websites.

If you would like to contribute to #GhostSec via donation you can visit http://crowdrise.com/operationisis or use our Bitcoin address found below. All donations received will go towards monthly server maintenance expenses and additional hardware to combat the Islamic State.

Ghost Security Bitcoin Address: 1KDkYapMUiwzHuCzNp32EGJY8c6eX6Hn6U

Your contributions to our cause are immensely appreciated and this could never be achieved without your unyielding support .

Ghost Security

We are the ghosts that you have created."

Upon examination of the electronic wallet mentioned in the publication, it can be seen that 0.274239 bitcoin coins (worth about $65) were transferred in the period of April through May, 2015.[148]

Worldwide Incidents of Information Leaks

Incidents of data and information leaks have increased in numbers and in the scope of information that is stolen and leaked. We see that there is an increase in theft incidents which were carried out as Cyber crimes, while there still a differentiation between personal data, financial information (including credit card details), medical information, and commercial information. Among the more significant attacks was the hack into the Office of Personnel Management and the

[148] https://blockchain.info/address/1KDkYapMUiwzHuCzNp32EGJY8c6eX6Hn6U

theft of private details of millions of US government employees. In a large number of the attacks, the scope of information stolen relates to millions of uses, while part of the information, such as financial or medical data, was sold on the black market and to forums on the Darknet. Personal information was sold for use in future attacks including blackmail and phishing attacks.

- According to a study published on May 27,[149] it seems that the average cost of a data breach is $3.8 million dollars, with average damages per lost or stolen records standing at $154 dollars. That is in comparison to $3.5 million dollars the previous year, and an average of $145 per record. The study looked at 350 companies from 11 countries that were harmed by information leaks, and found that aside from the direct costs incurred due to the breach damages, there were added expenses such as paying experts to repair the breach, investigate the incident, provide a hotline for customers, and monitor the credit cards activity of affected customers. The study claimed that the calculated average cost did not include mega breaches that affected millions of customers, such as the one involving Target – which alone incurred $148 million dollars in damages. The study also found that most of the information leak activity was carried out by organized crime elements who were well funded, and that the healthcare field was at the greatest risk. The cost of a breached record in that field stood at $363 dollars, as compared to the average of $154 dollars in all the other fields. And indeed, the health and medical field in the United States is a "Garden of Eden for Cyber criminals", who cause annual damage of six billion dollars, and steal 88.4 million records. Cyber criminals are increasingly focusing their efforts on attacking this field, because the information leaked and stolen is worth twenty times more than stolen credit data.
- On April 15, a repeated breach of credit information in several hotels owned by the White Lodging Services Corporation (WLSC) was reported.[150] The WLSC manages over 160 hotels in 21 states in the United States. On April 8 the company posted[151] an initial statement on its website, confirming the leak of credit card data from the food and drink vendors in ten of the chain's hotels, between July 3, 2014 and February 6, 2015. However, it was possible to learn from the statement that the company also suffered an earlier breach during 2014.

[149] http://www.reuters.com/article/2015/05/27/us-cybersecurity-ibm-idUSKBN0OC0ZE20150527?irpc=932
[150] http://www.ehackingnews.com/2015/04/white-lodging-confirms-second-data_15.html
[151] http://www.whitelodging.com/about/payment-card-issues

- On April 16, a report was published stating that the HSBC Finance Corporation announced[152] an information breach of its mortgage customers from some of its subsidiaries. The report was based on a letter[153] sent on April 10 from the company to the New Hampshire Attorney General's office. The letter stated that the company learned about the breach on March 27, and that the details of 685 customers from New Hamshire, accessing their accounts via the internet – most likely at the end of 2014. The information leaked included names, social security numbers, old account numbers, and telephone numbers.
- On April 20, a breach of the website of the Dead Sea Region Economic Company,[154] with leakage of the data base structure and hundreds of records, was reported. In addition, an information file from a breach of the "Municipal Support Site for Email and Online Calendar" of the Ramat Gan Municipality was breached.
- On May 15, the Penn State College of Engineering in the United States reported[155] that it had been the victim of two sophisticated cyber-attacks, and that at least one of them had been carried out by hackers based in China. An advanced randomware tool was used to for the system wide attack.
- On May 15, the University of Pittsburgh Medical Center (UPMC) reported[156] on its internet site that about 2,200 of its patients in the Emergecy Medica Care units received written messages informing them that they medical records may have been leaked to an external provider.
- On May 15, the MetroHealth System reported[157] a breach of three computers. The company was then forced to notify about 1,000 of its catheterization patients who had been hospitalized over the last year that their personal details may have been leaked. Already on March 17, the company noticed malware on three of its computers in the catheterization lab, which affected the patients in the lab between the dates July 14, 2014 through March 21, 2015. When the malware was discovered, it became clear that a second malware program had been present,

[152] http://www.net-security.org/secworld.php?id=18228
[153] http://doj.nh.gov/consumer/security-breaches/documents/hsbc-finance-20150410.pdf
[154] http://pastebin.com/GtfTAEv4
[155] http://news.psu.edu/story/357656/2015/05/15/administration/college-engineering-network-disabled-response-sophisticated
[156] http://www.upmc.com/media/NewsReleases/2015/Pages/mml-privacy-breach.aspx
[157] http://www.cleveland.com/healthfit/index.ssf/2015/05/metrohealth_reports_data_breac.html

and was only removed on March 21.

- On May 20, the CEO of Carefirst announced on the company website that the company had suffered a sophisticated Cyber attack,[158] during which the hackers had "gained limited, unauthorized access to a single CareFirst database". The incident affected 1.1 million current and former members, as well as individuals with business connections to the company who registered on the company's site before June 20, 2014.
- On May 21, it was reported that the FriendFinder dating site (based in the United States, with a branch in Britain) was hacked[159] and the personal details of 3.9 million customers were stolen. The information included sexual orientation and preferences, as well as whether or not the customer was interested in extramarital relationships. In addition, email addresses, names, birth dates, and unique computer and internet addresses were stolen. The information also included details about people who had requested to close their accounts on the site.
- On June 1, Japan's official authorities reported[160] that Japan's Pension Service was breached, and the details of 1.25 million citizens was leaked. The announcement claimed that computers used by the Pension Service staff had been accessed by an external email virus. The President of the Service apologized for the leak, which he said included names, ID numbers, birth dates, and addresses. He also stated that a special team had been established to investigate the cause, and the possible motivation for future attacks. At the same time, the Minister of Health and Welfare also apologized for the failure to prevent the breach, saying at a press conference that he had instructed the Pension Service to do everything in its power to protect the public's pensions.
- On June 5, another major breach of data was reported[161] by a US government source. This time there were about four million records that may have been stolen from the Human Resources Administration computers in the Interior Ministry. It seems that the incident occurred in December, 2014, but as was often the case in past instances, the breach was only discovered

[158] http://www.carefirstanswers.com/
[159] http://www.channel4.com/news/adult-friendfinder-dating-hack-internet-dark-web
[160] http://www.reuters.com/article/2015/06/01/us-japan-pensions-attacks-idUSKBN0OH1OP20150601
[161] http://www.independent.co.uk/news/world/americas/us-officials-claim-massive-breach-of-government-personnel-data-10298575.html

long afterwards – in April, 2015. On June 12 it was reported[162] that the number of records of current and former US government employees which were stolen from the Office of Personnel Management server could reach up to 14 million, and not 4 million, as was originally reported in the official OPM statement.[163] The new estimate was that the theft of between nine and 14 million records of government employees – mostly former employers or suppliers – started in the 1980's. That assumption was provided by two clerks involved in the investigation. This estimation was published one day after the claim that the theft was much more serious than it seemed at first, and it was determined that the hackers had stolen from the central database personal information and social security numbers of all the government employees. In a letter sent by the OPM, it was written that the assumption was that the hackers were able to place their get their hands on records which included addresses, birth dates, employment and payment histories, health insurance data, life insurance data, financial information, and even the age, gender, and ethnic group of the employees. The report claimed that the database contained 780 different types of information about most of the US government's civilian employees – those who were not members of Congress or staff. Therefore, a FAQ[164] page about this incident was published on the OPM website.

Cyber-crime in the United States Medical Arena

On May 7, the rising of Cyber attack against the Medical System in the United States was reported. Cyber criminals who were increasingly focusing on this field caused damages amounting to six billion dollars annually. [165]

The Cyber attacks against service providers in the medical field have more than doubled over the last five years, with damages averaging 2.1 million dollars per hospital, with 90% of the medical service providers in any one state affected by similar attacks of the last two years. Half of the attacks were criminal in nature. [The above data, as well as information in the text that follows,

[162] http://nr.news-republic.com/Web/ArticleWeb.aspx?regionid=3&articleid=43234662
[163] http://www.opm.gov/news/latest-news/announcements/
[164] http://www.opm.gov/news/latest-news/announcements/frequently-asked-questions/
[165] http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually

was reported in a study called "Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data Promotion",[166] which was recently published by the Poneman company.]

It has also become apparent that despite widespread awareness that these numerous incidents create, most entities are still not prepared to defend themselves against sophisticated Cyber attacks. And indeed, more than half of the organizations surveyed for this study reported that they do not possess the necessary technology to prevent hacks or to identify them quickly. They do not even have experts on hand with the required technical skills to deal with the phenomenon.

These attacks are carried out by Cyber criminals, and are for the most part extremely sophisticated. They choose to attack the medical databases because they information contained there is very valuable. And that is due to the fact that medical records usually contain social security numbers, addresses, and medical information – all of which increase the value of the data twenty times more than the data acquired from stolen credit databases. The stolen data is then used to help people secure loans, open credit lines on the names of the victims, or to steal the medical identity of one of the victims of the information theft in order to receive free medical treatment.

The study revealed that during the year 2014, 88.4 million records were leaked due to theft or breaches, which is double the number from 2010. This figure was based upon the obligation of any organization providing medical services to report to the Department of Medical Services any leaks involving the data of more than 500 patients.

Amidst the waves of attacks that damaged medical institutions in the United States, there were also other breaches: a total of 11 million records stolen from the Premera Blue Cross health insurance company, in March 2015; details about 4.5 million patients stolen from hospitals managed by the Community Health Systems, as reported in August 2014; leaked details of all 62,000 employees of the University of Pittsburgh Medical Center; and leaked data about 56,000 patients of public medical services in San Francisco.

[166] https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data

Ransomware

- According to the Symantic Company's June report,[167] during the months of April through June there were about one million attacks involving ransomware, though only about 7% of those attacks used malware encryption that encrypt a computer's files and require ransom in order to decrypt them. While there was a decrease in the number of attacks in 2015 as compared to the previous year, there was an increase in the number of attacks during June – a total of 477,000 attacks.
- In a report published by the Mcafee company in May 2015,[168] it was stated that in the first quarter of 2015 over 700,000 ransomware attacks were documented, with CTB-Locker and CryptoLocker being the most prevalent in the first quarter. According to the report, most of the attacks using CTB-Locker occurred in North America and Europe.
- At the beginning of May, a report was published about AlphaCrypt, a new ransomware activated through the TOR dark network. The malware drew on characteristics of the known ransomwares TeslaCrypt and CryptoWall.[169]
- It is estimated that the ransomware TeslaCrypt, a malware that attacked – among other things – computer files related to online games, collected payments of about $75,000 dollars during the period between February and April 2015 from 163 victims, via Bitcoin payments. Each victim had the choice of paying an amount between 0.5 and 2.5 Bitcoins (a value of about $550 dollars), or $1,000 dollars using a pre-paid card via PayPal.[170]
- On May 12, a report was released about the ransomware BitCryptor from the producers of CoinValut. This was a new and more advanced version of a ransomware, which was developed after the National High Tech Crime Unit (NHTCU) successfully took control of the control server (C&C) of the older version of the malware.[171]
- On May 23, a Dark Network site announced that anyone who wanted to could create ransomware for free. The owner of the site would receive a fee for the ransom received (20% of

[167] http://www.symantec.com/content/en/us/enterprise/other_resources/intelligence-report-06-2015.en-us.pdf
[168] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf
[169] http://www.webroot.com/blog/2015/05/04/alphacrypt/
[170] https://www.fireeye.com/blog/threat-research/2015/05/teslacrypt_followin.html
[171] http://news.softpedia.com/news/CoinVault-Authors-Release-New-Ransomware-481534.shtml

the total value of the ransom), with the user choosing the amount of ransom to demand (a minimum of $50 dollars), and the payment would be made using Bitcoins. This ransomware used TOR technology with the goal of connecting the C&C server.[172]

- On May 26 information was published about a ransomware used against Android phones, disguised as a message from the FBI. This ransomware demanded payment of $500 dollars.[173]

Coping with Cyber Threats

Many countries are increasing their investment and their willingness to cope with the threats in the Cyber realm, whether by amending laws or establishing institutions and bodies with the authority and responsibility to cope with such challenges.

- On April 1, the Wall Street Journal online reported[174] that Singapore had established a new office called "Cyper Security Agency of Singapore"[175] to deal with Cyber challenges. The office will focus on developing and implementing national Cyber security strategies. The Minister of Communication and Information, who is slated to serve as head of the new agency, said in May that cyber security breaches will "continue to make headlines around the world," and added that they are likely to become more frequent and more sophisticated. Singapore itself suffered from this phenomenon when the Prime Minister's official site was hacked in November, 2013.[176] Along with supervising Cyber security policies in the country, the new agency will cooperate with the country's growing Cyber security industry. Meanwhile, last September INTERPOL opened a facility in Singapore, for the purpose of global combat against Cyber crime, and in February this year, the FireEye Company inaugurated a new operations room in cooperation with the local telecom company Singtel. The Boeing Company also announced in September 2014 that its first Cyber office outside of the United States would be in Singapore.
- On May 17 a report was published[177] claiming that the British government secretly changed its

[172] https://blogs.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us
[173] http://www.scmagazine.com/spam-campaign-targets-android-users-in-english-speaking-countries/article/416737/
[174] http://blogs.wsj.com/digits/2015/04/01/singapore-launches-new-cybersecurity-agency/
[175] https://www.csa.gov.sg/
[176] http://www.wsj.com/articles/SB10001424052702303763804579184612994768626
[177] http://thehackernews.com/2015/05/anti-hacking-law.html?m=1

laws against online hacking, and thereby protected the GCHQ, the police, and the electronic intelligence agency from criminal prosecution in the case of their hacking into cellular phones and computers, for the controversial purpose of surveillance. Information about the change was revealed just hours before a scheduled hearing on the topic of the legality of hacking into the computers by the law enforcement authorities in Britain and the intelligence agencies. However, it was claimed that the government passed the law two months prior to the hearing, in contradiction to the Computer Misuse Act (CMA), and thereby gave the GCHQ and other intelligence agencies much more protection with the amendment to the laws that criminalize hacking. The new law, which allows these organizations to hack without fearing criminal prosecution, was passed on March 3, 2015, and went into effect on May 3. However, the British government denied the claims made by Privacy International,[178] and stated that it didn't make any changes to AMC that would affect the activities of the spy agencies.

- On May 20 it was reported[179] that the US Navy NAVAIR Cyber Warfare Detachment (CWD) asked private companies[180] to develop technologies to protect drones, missiles, sensors, unmanned vehicles, and airborne weapons from hackers. The strategy of the CWD is to secure access points to weapon systems (identification and prevention), ensure operational survival and continuity during face-to-face battle (resiliency and retaliation), and manage smart Cyber acquisition in order to achieve those goals. The foundations upon which the CWD strategy for the NAVAIR's weapon system stands are: the development of a Cyber work force; investment in infrastructure, research and development; setting rules and standards, and recommended work methods. However, for the time being this strategy won't even move past the recommendation stage until May, 2016, and it will take at least five years until full implementation takes place – during which time the systems are essentially unprotected.

Developments in International Legal Efforts to Combat Terrorism in Cyberspace

[178] https://privacyinternational.org/?q=node/584
[179] http://www.engadget.com/2015/05/20/us-navy-wants-hack-resistant-drones/?ncid=txtlnkusaolp00000595
[180] https://www.fbo.gov/index?s=opportunity&mode=form&id=6dd007eb4561583a583d66658e8f3c16&tab=core&_cview=0

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, ANF, 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, adopted 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's noting terrorists' use of 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[181] and the Global Counterterrorism Forum,[182] 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.

[181] http://www.un.org/en/terrorism/ctitf/wg_counteringinternet.shtml
[182] https://www.thegctf.org/

Case Study – #OpIsrael - 2015

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

On April 7, the OpIsrael 2015 cyber-attack reached its climax, as confirmed by elements that identify with the group "Anonymous" the end of December 14.[183] This was the third year in a row that the attack has been carried out on the same date. Despite the target date, the activity within the framework of the attack already started at least a week beforehand, and continued at a very low intensity for a while after that date passed. The height of activity was in the early morning of April 7, and it gradually decreased over the course of the day. It should be noted that the OpIsrael events occur throughout the year at different times, whenever the hackers see fit, and are not limited to April 7. When the campaign ended, a notification was published on the website[184] belonging to Anonyous, saying, "a number of hackers have decided to continue until April 20."

The Main Findings

Information Leaks

Most of the events reported were the publication of information that was supposedly leaked during hacks to different Israeli sites.

As in the past, in the framework of this project, those reports can be divided into a number of types, based on their frequency, from the most frequent to the very infrequent:

Information manipulation – Published information that has no significance, which is not an actual leak, and/or the source of which is not in a hack. In these cases, the source of the information is manipulation of data so that it will appear to be a leak of valuable information.

Publishing revealed information, and presenting it as leaked information – An example of this is within this project is the publication of a list of personal details about Israeli Parliament members, with the claim that it was leaked from the Knesset website. In fact, it was all publically revealed information about the members of the 18th Knesset, who completed their terms in October 2012.

[183] http://middleeasternet.com/?p=34372
[184] http://anonhq.com/opisrael-continues-20th-april

Credible information that is not updated – An example from this project would be the leaked details of 1,700 students from Ben Gurion University. At first glance, it appears that it is indeed information accessed through a hack into a database. But based upon Facebook responses to the article I wrote about the list, it appears that the list is two years old.

Credible, up to date information – Such instances are relatively rare, and it is presently difficult to estimate the scope of such publications.

Website Defacement

Many lists include websites that are clients of companies that build or store websites, and when the former are hacked, it is possible to get to all the other clients of the latter.

A sample study of the sites in the different lists revealed that most of them are functional or in the process of being built.

On some of the lists of sites that have been defaced, at first glance it isn't possible find anything common to them all with regard to who built or stored the site.

Some of the sites were not repaired and display the contents uploaded by the hackers even a week after the fact.

Hacks

The total amount of hacks, from among the entire gamut of events, was relatively low, and the lists of sites that were hacked often dealt with sites that were defaced.

The reports about hacks mostly referred to websites, and very few referred to hacks of other targets, such as Facebook accounts.

Attacks

There have not been any reports about coordinated attacks such as "denial of service" hacks, unlike in the past when such incidents were prominent. The only mention of such an incident was of announcement made time to time on Israeli government sites saying that the sites are not available – but with no connection to prior attacks, and with no claim of responsibility from anyone for "knocking out" a site.

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

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

Nir Tordjman, Team Research Manager, ICT

ICT Interns

Chantelle Berman

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.