Cyber-Desk Review: Report #2

The second cyber-desk report 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 has been linked to jihad (funding, methods of attack).

The report discusses the collaboration between the "Anonymous" group and Jihadist hackers in Electronic Jihad. The report highlights a chat software program specifically for Jihadists, as well as a number of security breaches by the "Al-Fallage Team". Key topics of Jihadist discourse and Jihadist propaganda are listed and include addresses by prominent Al-Qaeda leaders and the formation of new media outlets.

During the course of January 2013, several events were detected in the world of cyber-crime and cyber-threats to the world economy, banking and business. These attacks included data leaks from FBI servers, online attacks of malware, hacking the website of the Chamber of Commerce in France, and the threat of cell phone hacking. In Britain, Christopher Weatherhead and Ashley Rhodes were arrested for the execution of a series of online attacks.

This report's case study focuses on Iran's suspected involvement in the attacks on American banks. Also spotlighted in this report are the "Anonymous" group and their activities in the Middle East and against Israel.

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-attacks. The following is a selection of recent key acts of electronic jihad, and a brief overview of the key themes reflected in jihadist discourse and propaganda.

Collaboration between the Anonymous Group and Jihadists Hackers:

The "Al-Falllaga" Tunisian hacker group announced a new collaboration, the first of its kind, with the "Anonymous Tunisia" hacker group. The connection between the two was enabled, by a third party whose identity the group refused to disclose due to security reasons. According to the statement, the objective of this collaboration is to expose corruption in Tunisia through the publication of classified documents that shed light on this issue. It noted, for example, the intention to disclose documents showing the connection between the ruling party in Tunisia, headed by the Muslim Brotherhood's Al-Nahda Party, and the US, as well as the identity of the murderers of protestors in the Jasmine Revolutions.[1]

In addition to this collaboration, the "Al-Falllaga" announced another collaboration with a group of hackers called Kalashnikov, whose views align with the concept of global jihad.[2]

[1] December 31st 2012, https://www.facebook.com/FallaGa.tn#!/photo.php?fbid=526523610705388&set=a.397482876942796.98987.397481643609586&type=1&theater

[2] December 29th 2012, https://www.facebook.com/Kalachnikovtn#!/photo.php?fbid=316272448476964&set=a.311048688999340.64278.303102983127244&type=1&theater

From top to bottom: the logo of the Al-Fallaga Team and the logo of the Anonumous group

From right to left: the logo of the Al-Fallaga Team and the logo of the Kalashnikov group

Defensive Tactics

Communication program for Jihadists:

A supervisor of the Al-Minbar jihadi forum proposed the surfers use a chat program called Beyluxe Messenger. According to him, within the software can be found a chat room called: "The Supporters of the Al-Nusra Front", Al-Qaeda's affiliate in Syria.[3]

[3] December 15th 2012, http://www.alplatformmedia.com/vb/showthread.php?t=16640

Offensive Tactics

The "Al-Falllaga Team", a Tunisian hacker group, whose views identify with global Jihad, published throughout December 2012 a number of claims of responsibility for several security breaches on the net:

- Claimed responsibility for hacking several Israeli servers and websites, such as: http://horizontech.co.il/images/index.html.[4]

- Claimed responsibility for the attack on a number of servers in Myanmar in response for the policy of oppression led by the regime against the Muslims in the country.[5]

- Claimed responsibility for the hacking and takeover of Marcel Khalife's Facebook account, an oud (instrument) player of Lebanese origin, https://www.facebook.com/marcelkhalifereal.[6] According to the group, the breach occurred following a melody composed by Marcel to one of the Quran verses.

Marcel Khalife's Facebook account after having been hacked by the group

4 https://www.facebook.com/FallaGa.tn?ref=stream#!/photo.php?fbid=524622057562210&set=a.397482876942796.98987.397481643609586&type=1&theater ; https://www.facebook.com/FallaGa.tn.Nabeul#!/photo.php?fbid=523726117651804&set=a.397482876942796.98987.397481643609586&type=1&theater

5 December 25th 2012, https://www.facebook.com/FallaGa.tn.Nabeul#!/photo.php?fbid=523465367677879&set=a.397482876942796.98987.397481643609586&type=1&theater

6 https://www.facebook.com/FallaGa.tn

A member of the Hanein jihadi forum noted that a hacker called ABO aBYDa aL MaSReY hacked into a number of American websites to commemorate the anniversary of the Humam Al-Balawi's death, also known as Abu Dujana Al-Khurasani. Abu Dujana, a Jordanian doctor, perpetrated a severe terrorist attack against a CIA base in Afghanistan on December 31, 2009, killing seven American intelligence officers and a Jordanian officer. Amongst the American sites that were hacked were the following:[7]

http://www.rewards4sharing.com, http://www.jessicaallen.us, http://www.artcenterkorat.com, http://www.renbuilder.com, http://www.daboyzsports.com, http://www.georgedeshields.com, http://www.myrjsphotography.com, http://www.tbsdevdemo.com, http://www.cherylsmithonline.com.

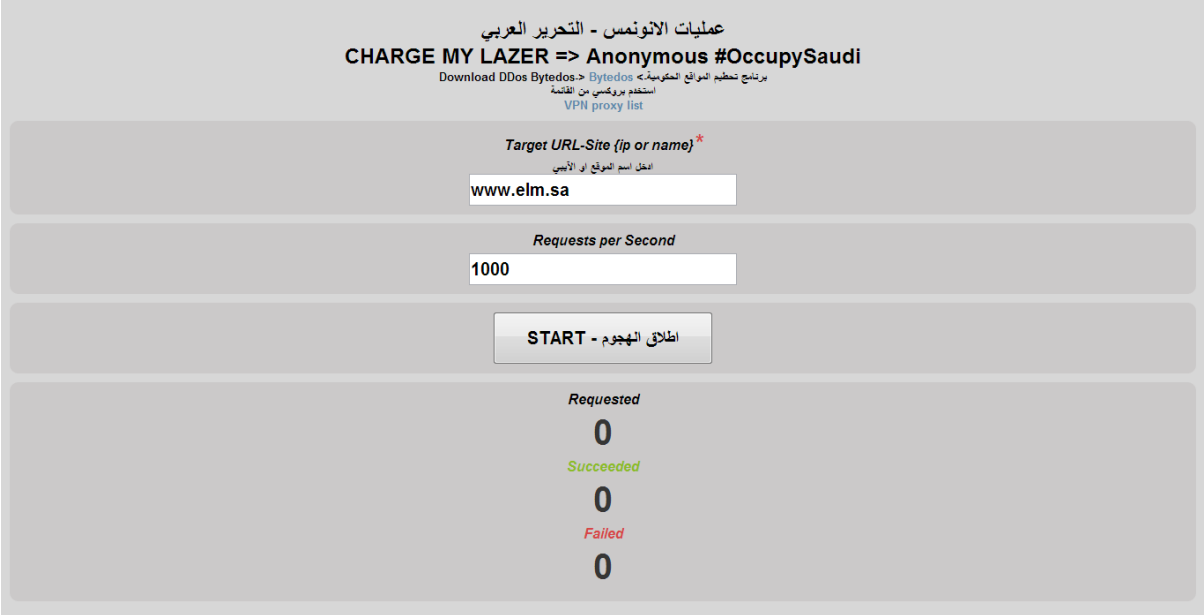
Abu Dujana's photograph posted on the Al-Hanein forum

[7] December 30th 2012, http://www.hanein.info/vb/showthread.php?t=307252

A banner planted by the hacker in the American websites hacked in memory of Abu Dujana

"The Arab Anonymous Group for Opposition against Arab Tyranny, Global Imperialism, the Freemasons and Zionism" called on December 6, 2012 to attack various Israeli websites as well as an extensive list of Arab websites such as the Ministry of Interior of Kuwait, Saudi Arabia, Libya, Egypt and more. To that end the group asked the surfers to enter the web address http://pastehtml.com/view/cc8nfn50e.html and enter in the appropriate line the names of the relevant websites. This call was posted on the Twitter account called "The Electronic War" https://twitter.com/AnonArabOps.

The group's logo on the Twitter account



The website where the surfers were asked to enter Saudi website addresses in order to take them down off the net

Key Topics of Jihadist Discourse, and Jihadist Propaganda, December 2012

1. An old video tape containing an address made by Sheikh Al-Zawahiri to the Egyptian Salafi Sheikh, Hazam Saleh Abu Ismail, to concentrate efforts in order to complete the revolution in Egypt.

2. Sheikh Khaled Bin Abdel Rahman al-Hussainan aka Abu Zayd Al-Kuwaiti, a senior Al-Qaeda member, was eliminated by drone fire.

3. Al-Rubaysh, Al-Qaeda in the Arabian Peninsula's Mufti, criticized the submission of Muslims and the absence of appropriate responses on their part to the US's aggression. The Muslims, according to him, are obliged to adopt an approach of activism against their enemies.

4. Al-Qaeda in the Arabian Peninsula offered a monetary reward for anyone who eliminated the US ambassador in Yemen and American soldiers on its land.

5. Al-Wadud, leader of Al-Qaeda in the Islamic Maghreb, clarified that anyone taking part in an attack on northern Mali and anyone taking part in its planning would be subject to severe retaliation on the part of the organization. He called on African countries not to cooperate with the France invasion plan in northern Mali as it only cares for its own interests and not for theirs.

6. A new Salafi jihadi group called Ansar Al-Sharia declared its founding in northern Mali.

7. The Al-Tawhid wal-Jihad group in West Africa declared the establishment of a new jihadist media institution named "Al-Murabitoon".

8. The Salafi jihadist in Egypt called to boycott participation in the referendum for the establishment of Egypt's new constitution.

9. A new Syrian Islamist umbrella organization called "The Syrian Islamic Front" declared its establishment on December 21, 2012, as well as its intention of turning Syria into an Islamic theocracy.

10. Sheikh Abu Harith Al-Maqdisi, a member of the Ansar Al-Sharia Army in Syria, discussed his vision for the day after the fall of Bashar Al-Assad. The Mujahideen would turn toward Jordan, conquer it, and turn it into an Islamic theocracy. Lebanon's Hezbollah would have to fight for its life, and the threat to Israel's security from the Mujahideen would intensify.

11. The Al-Shabab Al-Mujahideen movement in Somalia announced that Sheikh Abu Mansur Al-Amriki was no longer a member of the group because of his attempts to divide the ranks of the Mujahideen by spreading fallacious reports, which have been widely covered by the Western media, that there are deep rifts within the leadership of Al-Shabab.

12. Three leading jihadi forums, the Shumukh Al-Islam, Al-Fida and Ansar Al-Mujahideen, stopped operating on the web at the beginning of December 2012, returned to activity on December 18, 2012, and stopped operating once again a few days later. According to the members of the other jihadi forums this was another component in the war waged by the enemies of Islam against the Muslims and Islam.

Cyber-Crime and Cyber-Terrorism, January 2013

In the course of January 2013, the following events were detected in the world of online crime and online threats to the world of economy, banking and business:

Data Leaks:

- In the scope of an ongoing extensive operation of entities identified with "Anonymous", a breach was made into the Asian Bankers Associates website.[8] The entire website's database was exposed, including user names and passwords of the website administrators and its users as well as the structure of the database.[9] The user's data included: a definition of the type of membership, the bank the user belongs to, the country, the type of bank and email address. A similar breach was carried out into the following financial sites:

  https://www.americanfinancing.net, http://www.coinsandcanada.com, http://www.dancham.or.th

- On January 6, 2013 a breach of the ic.fbi.gov domain was reported, an event in the course of which the user names and passwords of 293 of the organization's employees were stolen and leaked. It should be noted, on October 19, 2012 another breach was reported to the FBI servers (ns1.fbi.gov) in the course of which details on the data base was exposed as well as the user names and passwords of about 300 of the organization's personnel.[10]

[8] http://www.aba.org.tw
[9] The notice page is no longer available. http://pastebin.com/hULqUEtA
[10] GUEST, "FBI Email leak ic.fbi.gov,", Pastebin, JAN 6TH, 2013 http://pastebin.com/77Ukzq4s

Online Attacks:

On January 16, 2013 online activity was reported, consisting mainly of fake emails on behalf of the Europcar car rental company. These emails included a zip file attachment titled EuropCar Invoice.zip constituting malware which upon its activation allows its senders to in fact control the destination computer and even steal data from it.[11]

Hacking Sites:

On January 27, 2013 it was reported that the Chamber of Commerce website in France[12] was hacked and vandalized by a Tunisian group of hackers called the Tunisian Cyber Army. The information[13] was given on the group's Twitter account and included a shot of the screen[14] of the vandalized page and details as to the manner of hacking to the site using the SQL Injection method. It is important to note that the problem such hacking can cause is not necessarily the vandalizing itself. Once the hackers succeed in entering the site, they can change the homepage and vandalize it, but they can also get their hands on the website's database, and disrupt, steal and leak data contained therein.

Cellular:

In an article in Russian it was claimed that local hackers would soon have the ability to takeover users' cell phones, disable them from afar and demand ransom in return for releasing the blocked phone. In addition, such hackers can use payment programs installed on the victim's cell phone and remotely carry out various transactions while charging the victim's payment details.

Arrests:

In the course of the month a report was given on the arrest of two young men in Britain, Christopher Weatherhead and Ashley Rhodes, for the execution of a series of online

[11] Graham Cluley, "Beware! Malicious Europcar invoice emails spread Trojan horse attack,", Naked Security,
http://nakedsecurity.sophos.com/2013/01/16/malicious-europcar-invoice-trojan
[12] http://www.cci.fr
[13] TunisianCyberArmy1, Twitter, 6:37 PM - 27 Jan 13
https://twitter.com/TN_cyberarmy/status/295571244768698369
[14] TunisianCyberArmy1, Twitter, 6:37 PM - 27 Jan 13
https://twitter.com/TN_cyberarmy/status/295571244768698369/photo/1

attacks against the PayPal payment service in the course of December 2010, as well as against the MasterCard and Visa credit card companies. This was part of the activity carried out by "Anonymous" against these companies who refused to transfer funds connected to the WikiLeaks site. It was claimed that these attacks caused these companies damages estimated at millions of dollars.[15]

[15] Dow Jones Newswires, "Anonymous Hackers Jailed over PayPal Attack,", FOX News Network, January 24, 2013
http://www.foxbusiness.com/news/2013/01/24/anonymous-hackers-jailed-over-paypal-attack/

Case Study

Is Iran behind the attacks on the American banks?[16]

In the course of September – October 2012, the financial system in the US was under a cyber-attack exceptional in its scope and intensity, whose aim was to impair the normal online operations of many of the larger banks in the US. What makes these recent attacks on the financial system unique? Why did the subject reach the headlines with such force? An examination of the events in the cyber world alongside the events in the "real world" and the statements made by senior government officials in the US points to the possibility of it being an attack, timed and coordinated by a state entity, possibly Iran. If this is indeed the state of affairs, this is an escalation in the cyber threat, which until today we have only seen the tip of its iceberg. The conclusion – the rules of the game are changing and those who are quick to understand that the threats in the virtual reality are tangible, sophisticated and changing with extreme velocity, will increase their chances in defending themselves in face of a future attack.

Today, more than half of cyber-attacks are on financial organizations[17] and the threat increases daily. The reasons for this are numerous, including: hacking into bank computers as a personal challenge for hackers, stealing money, fraud, extortion, espionage or to cause functional damage. These attacks, in all of their variety, occur every day, at an almost inconceivable rate, in an increasing level of sophistication. Most of the organizations and hackers are mainly concerned with money theft, identity theft, stealing sensitive and even confidential information. The importance of the financial sector alongside its dependence on computers makes it extremely susceptible to the destructive threat, even more when the motives of the attackers are not financial, or in case of the financial system when the aim is to disable the bank and not steal money from it. The US Secretary of Defense, Leon Panetta, referred to this matter in his speech

---

[16] By Ram Levi ramlevi@tau.ac.il, cyber advisor for the National Council for Research and Development, and researcher at the Yuval Neeman Workshop for Science, Technology and Security at the Tel Aviv University.
This review was prepared with the help of
Lior Tabenski – researcher at the Yuval Neeman Workshop for Science, Technology and Security at the Tel Aviv University
Advocate Dvora Housen-Kuriel – fellow at the Yuval Neeman Workshop for Science, Technology and Security at the Tel Aviv University
Motti Geva – doctoral student for Information Security at the Bar Ilan University

[17] Check Point. *Check Point Survey Reveals More Than Half of Targeted Attacks Reported Were Driven by Financial Fraud.* May 22, 2012. http://www.checkpoint.com/press/2012/052212-check-point-survey.html (accessed October 12, 2012).

last November, saying:[18] "Cyber-attacks perpetrated by nation states or violent extremists could be as destructive as the terrorist attacks on 9/11. Destructive cyber terror attacks could virtually paralyze our nation".

As an example, Panetta referred to the attack called "Shamoon" that erased approximately 30,000 computers of the Aramco Saudi gas company and causing similar damage to the "RasGas" company, as "probably the most destructive attack on the private sector thus far".[19]

One cannot exaggerate the serious implications of a similar attack on the financial sector. The financial sector is based on the public's trust, believing that financial information and its funds will be available. The potential realization of increased threats, along with a growing dependence on information available online, the cyber threat becomes a risk factor for strategic, operational and image for each bank individually and to the financial sector as a whole.

A survey conducted by Guardian Analytics[20] last May amongst small and medium sized businesses (SMBs) in the US found that 20% of the organizations carry out all of their banking activity online and that 50% carry out more than half of their banking activity online. Most of the organizations surveyed view, and justly so, the financial system as bearing most of the responsibility for securing their financial information and funds. More interesting is that two thirds of the organizations discovered they were victims of financial fraud. However, what should trouble the banks most is that businesses that were victims of financial fraud transfer the bulk of their business activity to another bank. The great majority, according to the survey, will do so after one single event. It is therefore no wonder that financial institutions, including the banks, invest enormous amounts of resources in information security which is the core of their activity. It is no wonder that the attack that began last September drew such attention.

One of the most available and common methods for disrupting the availability of websites and online services is a "Distributed Denial of Service" attack (DDoS). These attacks began at the late 1990s (1999) and since then have become more elaborate. Today the most common and inexpensive technique is using the Botnets network. This network is built by the insertion of malware (Bot) to tens of thousands of personal computers dispersed around the world, without the users' knowledge. Thus, the attacker can control remotely these computers and at any given time give them an order to go to

[18] Panetta, Leon. *Defending the Nation from Cyber Attack.* October 11, 2012. http://www.pentagonchannel.mil/Video.aspx?videoid=158228 (accessed October 14, 2012).
[19] See on the matter, the test case published in newsletter no. 1.
[20] Guardian Analytics. *2010.* May 2012. http://info.guardiananalytics.com/2012TrustStudy.html (accessed October 18, 2012).

a website or any other online service until the servers themselves or the servers' network cannot cope with the overload and stop providing service.[21] An organization that is technologically inferior wishing to perpetrate such an attack does not have to construct the network itself but rather hires DDoS services for the period of time necessary for perpetrating the attack. For example, this is what the "Saudi Hacker" did.[22] This is a cheap and simple attack to carry out, when defending against it is an expensive matter. For the sake of illustration, American companies view the prevention of normal services as a significant threat and a successful attack on these services costs these organizations, on average, about a quarter of a million dollars.[23]

"The Ababil Operation"

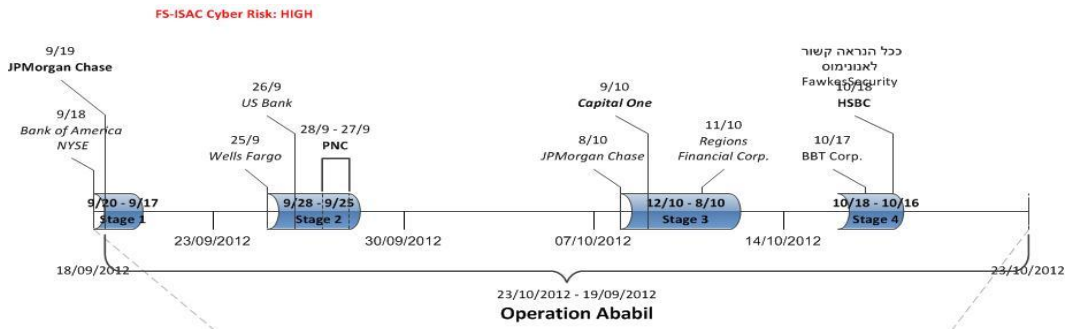
On September 19, 2012 the Information Sharing and Analysis Center of the American private sector (FS-ISAC) raised the threat level of cyber-attacks on the financial sector from medium to high, the second highest level of threat. Raising the level of threat was based on "reliable intelligence" on cyber-attacks on American financial institutions.[24] A day beforehand, the FBI, FS-ISAC and the IC3[25] (the Internet Crime Complaint Center), also published a high alert to American banks regarding a focused and significant threat of cyber-attacks, including for the purpose of stealing funds.[26] The publication referred explicitly to the fact that in order to gain access to the banks' networks, the attackers would employ a sophisticated fraud, with several methods of automated attacks simultaneously, as well as gather intelligence through "social engineering". Alongside these alerts, they warned against cyber-attacks whose aim was to impair the banks' functioning as well as against a significant rise in the complexity of the Distributed Denial

[21] Hence the name of the attack – "Distributed Denial of Service" attack or DDoS.
[22] See on the matter: Levi, Ram; Housen-Kuriel, Dvora. "The Saudi Hacker" – *A New Age in the Israeli Cyber Space*, January 13th 2012. http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1665, (accessed February 18, 2013).
[23] Check Point. Check Point Survey Reveals More Than Half of Targeted Attacks Reported Were Driven by Financial Fraud. May 22, 2012. http://www.checkpoint.com/press/2012/052212-check-point-survey.html (accessed October 12, 2012).
[24] FS-ISAC. *Financial Services - Information Sharing and Analysis Center.* October 18, 2012. http://www.fsisac.com/ (accessed October 18, 2012).
[25] IC3 – the Internet Crime Complaint Center. A collaboration between the FBI and the White Collar Crimes Center in the US. See: http://www.ic3.gov/default.aspx
[26] FBI, FSISAC, IC3. "Fraud Alert – Cyber Criminals Targeting Financial Institution EmployeeCredentials to Conduct Wire Transfer Fraud." *http://www.ic3.gov.* September 17, 2012. http://www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf (accessed October 2012, 2012).

of Service attacks[27] that would exploit a large number of weaknesses that were recently discovered and are incorporated in the attack tools used by the attackers.[28]

The day beforehand, on September 18, 2012 the "Izz Ad-Din Al-Qassam Cyber Fighters" organization published that it intends to harm assets important to the US and to disrupt the activity of the financial system in the US so as to bring about the erasing of "The Innocence of the Muslims" movie[29] – the movie that ignited the violent outbursts of Muslims worldwide following its broadcasting on September 11, 2012.[30] In a notice published by organization it was stated: "The Muslims must do all they can to stop the distribution of the movie". During the weeks that followed, many banks were attacked by the organization in a coordinated and synchronized operation – "The Ababil Operation".[31]

The attack began with the prevention of the online services of the Bank of America[32] (the second largest bank) in the US and the prevention of services of The New York Stock Exchange[33] website. The attackers warned that the attack may come in different ways.[34] A day later the JP Morgan Chase website, belonging to the largest bank in the US, was attacked.



Drawing no. 1 – the timeline of the Ababil Operation. Source: Ram Levi

[27] In English: Distributed Denial of Service (DDoS).
[28] Cisco. *Cyber Risk Report - September 17–23, 2012.* September 23, 2012. http://www.cisco.com/web/about/security/intelligence/CRR_sep17-23.html?vs_f=Cyber%20Risk%20Reports&vs_cat=Security%20Intelligence&vs_type=RSS&vs_p=September%2017-23,%202012&vs_k=1 (accessed October 18, 2012).
[29] Cyber fighters of Izz ad-din Al qassam. *http://pastebin.com.* September 18, 2012. http://pastebin.com/mCHia4W5 (accessed October 12, 2012).
[30] The New York Times. *The 'Innocence of Muslims' Riots (Nakoula Basseley Nakoula).* October 22, 2012. http://topics.nytimes.com/top/reference/timestopics/subjects/i/innocence_of_muslims_riots/index.html?s=oldest& (accessed October 18, 2012).
[31] Ababil – swallow in Farsi, as well as the name of a drone manufactured by Iran.
[32] In proximity to the events, the Bank of America published on September 20th 2012 that it is seeking a Contractor, Cyber Forensic Investigator, Technology Infrastructure (6 months).
[33] Ibid, **Error! Bookmark not defined.**.
" Muslims worldwide must unify and Stand against the action, Muslims must do whatever is necessary to stop spreading this movie. We will attack them for this insult with all we have."
[34] QASSAMCYBERFIGHTERS. *Bank of America and New York Stock Exchange under attack unt.* September 18, 2012. http://pastebin.com/mCHia4W5 (accessed October 18, 2012).

A week later the Wells Fargo, US Bank and PNC banks were attacked.[35] On the second week of October, after a break of a week and a half, the attack continued against JPMorgan Chase, Capital One, SunTrust Banks, Regions Financial Corps, and a week after that the BBT Corp and HSBC banks were attacked (it is possible that the Anonymous Group was involved in the attack on the last bank).

Rank	Institution Name	Total Assets 06/30/2012	
1	**JPMORGAN CHASE & CO.**	$2,290,146,000	**Attacked**
2	**BANK OF AMERICA CORPORATION**	$2,162,083,396	**Attacked**
3	**CITIGROUP INC.**	$1,916,451,000	**Attacked**
4	**WELLS FARGO & COMPANY**	$1,336,204,000	**Attacked**
5	GOLDMAN SACHS GROUP, INC., THE	$948,981,000	
6	METLIFE, INC.	$825,188,490	
7	MORGAN STANLEY	$748,517,000	
8	**U.S. BANCORP**	$353,136,000	**Attacked**
9	THE BANK OF NEW YORK MELLON CORPORATION	$330,490,000	
10	**HSBC NORTH AMERICA HOLDINGS INC.**	$317,482,381	**Attacked**
11	**PNC FINANCIAL SERVICES GROUP, INC., THE**	$299,712,018	**Attacked**
12	**CAPITAL ONE FINANCIAL CORPORATION**	$296,698,168	**Attacked**
13	**TD BANK US HOLDING COMPANY**	$207,333,395	**Attacked**
14	STATE STREET CORPORATION	$200,368,976	
15	ALLY FINANCIAL INC.	$178,560,000	

[35] http://pastebin.com/izrLhERu

16	BB&T CORPORATION	$178,529,372	**Attacked**
17	SUNTRUST BANKS, INC. (1131787)	$178,307,292	**Attacked**
18	PRINCIPAL FINANCIAL GROUP, INC.	$152,050,658	
19	AMERICAN EXPRESS COMPANY	$146,890,000	
20	AMERIPRISE FINANCIAL, INC. (2433312)	$135,271,252	
21	RBS CITIZENS FINANCIAL GROUP, INC. (1132449)	$129,313,757	
22	REGIONS FINANCIAL CORPORATION	$122,344,664	**Attacked**

Drawing no. 2 – rating of the holding companies. Source: (Federal reserve 2012)

On September 23, 2012 in an interview to the C-Span network, the democratic Senator Joe Lieberman accused Iran of being behind the attacks (C-Span 2012).[36] Furthermore, the JP Morgan Chase Chairman stated in a speech given before the Council on Foreign Affairs last October as follows:[37]

> "[D]enial of service… they're flooding the lines… a lot of this is coming out of Iran. They're flooding the lines so that you can't get through".

On that same day, Gholam-Reza Jalali, Head of Iran's Civil Defense Organization, was quick to deny Senator Lieberman's accusations stating that "Iran did not hack into the American banks".[38] In truth, Jalali did not lie, Iran did not hack the banks as the banks were not hacked into, but rather were prevented from providing online services. In a more general manner, Jalali knows well that it is difficult to locate with certainty the source of cyber-attacks[39] due to the Problem of attribution, the difficulty to locate the source of the attack with certainty and attribute it to a specific entity. It is therefore very easy to deny that Iran was the one who attacked and very difficult to prove otherwise. Iran, who was a target for some of the most sophisticated cyber-attacks, is well aware of this fact.

---

[36] "http://Chase.com is experiencing intermittent issues. We're working to restore full connectivity & apologize for any inconvenience."
[37] Council on Foreign Relations. *The State of the Global Economy.* October 10, 2012. http://www.cfr.org/economics/state-global-economy/p29251 (accessed October 18, 2012).
[38] Fars News Agency. *Iran Rejects Media Reports on Hacking US Banks.* September 23, 2012. http://english.farsnews.com/newstext.php?nn=9106241736 (accessed October 12, 2012).
[39] See on the matter: Levi, Ram. The Fifth Battle Zone. Israel Defense www.israeldefense.co.il/?CategoryID=512&ArticleID=1470

What distinguishes the Ababil Operation?

As stated above, due to the problem of attribution it is difficult to identify with certainty the source of the attack. However, in an orderly process of finding computerized evidence (cyber forensics), including an analysis of the data from computers used for the attack, an analysis of the traffic, the method of operation, a comparison between the attacks, intelligence, motivation, the context of the attack, etc. it is possible to formulate assumptions regarding the entities behind the attack and to try and learn whether this was a state entity, a criminal organization or hackers.

The idea of preventing service is not a new one, but the method of execution was new and requires deepening briefly. As stated, usually Denial of Service attacks use compromised computers that burden the online service with a huge quantity of idle requests, until it crashes. The downside of this attack is that it requires a very large number of computers distributed worldwide, and controlling them is more complex. Naturally, personal computers have a relatively narrow bandwidth and therefore the amount of traffic they generate is limited in advance. In this case, use is made of a new attack suite (toolkit) called itsoknoproblembro (the name is funny but the attack is very serious). This toolkit uses compromised servers (called BRO-bots) where the attack command is "pushed" in a different manner than a bot network, where the computers "pull" the command – which makes early detection of the malware difficult, as it only listens, and does not carry out any action until the moment it is required to do so. Furthermore, because the servers usually have more traffic volume at their disposal (and significantly so), they can be used for the attack, which enables the causing of greater damage with fewer computers.[40] And with fewer computers, the control is better, and flexibility at the time of attack is greater.

This attack was exceptional in its scope and caused traffic in volumes exceeding 65Gbps. For the sake of comparison, attacks that are considered large scale are in the volume of 10Gbps. To manufacture such an attack, a smart and sophisticated attack network is required. It is no wonder that they succeeded in surprising the American banks (one can assume they prepared for serious Denial of Service attacks). The volume of traffic of the attack and the fact that the banks found it difficult to defend themselves against it indicates an organization with resources.

The motivation for the attack was radical Islam but there was no uniformity on the methods of attack between the banks. The method of attack employed by the "Izz Ad-

[40] Prolexic. *Intense 20 Gbps DDoS attacks became the new norm in Q3 2012.* October 17, 2012. http://www.prolexic.com/knowledge-center-ddos-attack-report-2012-q3.html (accessed October 18, 2012).

Din Al-Qassam Cyber Fighters", according to them, did not appear in the communication analyses of the attacks. There can be a number of explanations to this fact: the first, they intentionally misled the banks and the information security companies, so as to surprise them. The least likely explanation is that hackers tend to publish in advance the date and method of the attack so as to enlist supporters to help them (crowd hacking). Another possibility is that they are merely the face of the attack, and that the attack was in practice carried out by another entity in collaboration with them, or that they used tools that were not published. At this point there is also the possibility that the organization itself does not exist and is merely a front for political activity. It is hard to tell. In any event, this attack was more advanced and complex than the capabilities of a small organization – the type of attack that requires significant technological abilities that are usually found in crime organizations or in countries. The Akamai Company that provides 15-30% of the internet traffic worldwide also claimed that the attack could have been perpetrated by Iran, by Jihadi activists or by east European crime organizations.[41]

"The attackers and their motives have been linked to everything from cyber-Jihadi hacktivism to Iran-sponsored cyber war to Eastern European organized crime".

In other words, the too cannot tell.

The Iranian angle

The organization claiming responsibility for the attacks calls itself the "Izz Ad-Din Al-Qassam Cyber Fighters" and operates under the name the "Qassam Cyber Fighters". In the event Iran was the one behind the attacks it probably did so using the Quds Force – the Special Forces in charge of spreading the Islamic revolution at the Revolutionary Guards. The Quds Force has a long history of supporting organizations such as Hezbollah to execute terror attacks on its behalf, and they are well based in the Shiite communities around the world.[42] Iran, who was under the most sophisticated cyber-attacks in the world (Stuxnet, Flame, etc.) established cyber defense and attack forces. James Clapper, Head of the DNI, said in connection with the Iranian cyber capabilities at the Senate's Intelligence Committee last January that Iran's offensive cyber capabilities (against the US) have dramatically improved both in their depth and in their complexity in recent

[41] Smith, Michael. *Information, not Hope, is the Key to Surviving DDoS attacks.* October 1, 2012. https://blogs.akamai.com/2012/10/information-not-hope-is-the-key-to-surviving-ddos-attacks.html (accessed October 18, 2012).
[42] Congress. *Suspend the Rules and Pass the Bill, H.R. 3783, With Amendments*.house.gov. September 14, 2012. http://docs.house.gov/billsthisweek/20120917/BILLS-112hr3783-SUS.pdf (accessed October 18, 2012).

years. He estimates that the government and even the supreme commander have reached the conclusion that Iran can afford to attack the US using cyber measures.[43]

In November 2011 Iran established a defensive cyber headquarters to protect its critical infrastructures. Last February, Gholam-Reza Jalali, Head of Iran's Civil Defense Organization, announced that Iran is forming a defensive cyber army to protect the critical military networks.[44] Iran did so in response to the American cyber armament – if the US is reducing its forces and increasing its cyber forces, Iran will naturally do the same.

In June 2012 the Mehr News Agency reported that Iran was preparing a strategic plan whose objective is to protect Iran against future cyber-attacks.[45] Iran has recently signed a science research collaboration agreement with North Korea in this field, and has even proposed to help the countries increase their level of cyber defense.[46] Despite many declarations from Iran that it is not developing offensive cyber abilities, this is untrue. There are assessments that the Revolutionary Guards have a cyber-fighting unit. The assessments speak of the unit being comprised of approximately 2,400 people with a budget of 76 million dollars in 2010. In 2010 the Iranian Chief of Staff said that this is the second largest cyber army in the world. This statement leads to the possible conclusion that the army is employing hackers who carry out activities on its behalf, called the Iranian Cyber Army.[47]

The connection between them is unclear but this organization has carried out in the past extensive offensive activities against several international organizations.

In August 2011 the army falsified certificates and succeeded in penetrating tens of thousands of Gmail accounts. Using the Cyber Army, the government controls the content on the internet, especially on social websites, YouTube, etc. The Iranian Cyber Army, together with the Cyber Command, filters content and hacks into online sites and services that have computerized access,[48] so as to prevent the "soft war" against Iran.[49]

---

[43] James Clapper, testimony before the Senate Select Committee on Intelligence, January 31, 2012.
[44] Press TV. *Iran set to build first cyber army.* February 20, 2012. http://www.presstv.ir/detail/227739.html (accessed October 12, 2012).
[45] Mehr. *Iran is formulating strategic cyber defense plan: official*. June 15, 2012. http://www.mehrnews.com/en/NewsDetail.aspx?NewsID=1627386 (accessed July 12, 2012).
[46] [46] IRNA. *Cooperation to Upgrage Cyber Defense Level.* October 12, 2012. http://www.irna.ir/en/News/80369840/Politic/Iran_welcomes_int%E2%80%99l_cooperation_to_upgrade_cyber_defense_level (accessed 18 October).
[47] Center for Strategic and International Studies. *Cybersecurity and Cyberwarfare - Preliminary Assessment of National Doctrine and Organization.* 2011. http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf (accessed July 18, 2012).
[48] Ibid.

Last July a "senior official entity" at the Iranian cyber headquarters suggested the US take seriously the Iranian doctrine of "an eye for an eye"; "The Iranian Republic have high [attack] capabilities, and it will respond to the [American] war mongering". Iran understood that this area is critical in modern warfare.[50] "Cyber warfare is more dangerous than physical warfare" noted Brigadier General Abdullah Araki, Deputy Commander of the Revolutionary Guards.[51] A few days later, in September, the Commander of the Navy Forces at the Revolutionary Guards, Admiral Ali Fadavi, announced that the Iranian cyber forces had penetrated the enemy's classified information systems. He did not mention the exact networks nor who the enemy was that was breached, but his statement at the inauguration of the Navy's new Communications, Command and Control Systems is worth attention:[52]

> "The information (cyber) security is like a master key for the IRGC and it should receive the top priority".

Moreover, last February, Brigadier General Muhammad Hussein, counted and said that the Revolutionary Guards' cyber unit is "amongst the top four in the world".[53]

Iran is well aware of the attribution problem of cyber-attacks. To wit, Iran has threatened a number of times that if its nuclear installations are attacked, it will retaliate with a bombing of the American bases at the Gulf and with missiles on Israel. Iran's uranium enrichment facilities have been attacked with a virus (Stuxnet) and despite the fact that Iran openly blamed Israel and the US for the cyber-attack on its nuclear facilities it did not deliver on its threats. One can assume this is because it cannot prove beyond a shadow of a doubt who attacked it. The same attribution problem that worked in favor of the cyber attackers on Iran, now works in favor of the Iranians in the attacks on the banks in the US, if indeed Iran is the perpetrator. Iran has the motivation, the knowhow and the ability, but one must remember that because of the attribution problem, the Iranian connection with the Ababil Operation is merely speculation.

---

[49] Mehr. *IRGC releases details about BBC activities inside Iran*. February 25, 2012. http://www.mehrnews.com/en/NewsDetail.aspx?NewsID=1543269 (accessed July 20, 2012).
[50] Press TV. *Iran to give crushing response to US cyber attacks: Iran official.* July 25, 2012. http://www.presstv.ir/detail/227739.html (accessed October 12, 2012).
[51] Press TV. *IRGC ready to counter enemy's soft and hard wars: Iran cmdr.* September 25, 2012. http://www.presstv.com/detail/2012/09/25/263490/irgc-ready-to-counter-enemys-war/ (accessed September 26, 2012).
[52] Fars News Agency. *Commander: Iranian Cyber Forces Easily Access Enemies' Highly Classified Info.* September 30, 2012. http://english.farsnews.com/newstext.php?nn=9106243142 (accessed October 12, 2012).
[53] IRNA. *IRGC Among Top Four Cyber Armies of the World".* February 2, 2013. http://www.irna.ir/en/News/80525582/Politic/IRGC_among_top_four_cyber_armies_of_world (accessed February 3, 2013)

Summary

"Distributed Denial of Service" attacks (DDoS) are becoming more and more complex. The attackers have become more sophisticated and are using methods of attack that make it difficult for information security companies to find effective solutions. The network administrators have limited knowledge in the field and the problem is becoming more complex. The Denial of Service attacks are starting to have characteristics of what is known as an "Advanced and Persistent Threat" as they are more focused and are tailored exactly to the systems of the organization under attack. The new tools allow a calibration of the attacks once they begin more quickly, thus hampering the defense efforts.

The methods of defense customary today are divided into two main types: the cat and mouse approach, and the creation of traffic rules in order to cope with illegitimate traffic. The first approach is applied by increasing the bandwidth to a volume larger than the estimated threat. The problem is that the bandwidth costs the organization a lot of money and most of the time is unused. In the event of smaller organizations, they can be stored with larger suppliers (such as Google, Amazon, etc.) and then enjoy a collective bandwidth.

In the second approach, the network manager or the information security company providing protection services against Denial of Service attacks, insert ad-hoc rules to bring down the communication from the computers in which the attacks come from, or they are inputted into the system when a new attack is detected. The problem is that in some of the cases the attackers can use the computers of legitimate clients and these will not be able to receive service through no fault of their own. When the attack is highly distributed, it becomes even more complicated, as the attacked organization finds it hard to create "elastic" rules as a smart attacker knows how to generate multiple rapidly changing IP addresses. All this is assuming the pattern of the attack is known in advance.

The private sector is at the forefront of the war in the cyber space, alongside countries and state organizations. The cyber-attacks are becoming more complex and sophisticated and the Ababil Operation is an example of this. The banking system is an attractive target for attackers, and safeguarding the proper functioning of the financial system is of the utmost importance in protecting financial stability and security. It seems that things are only getting worse. The array of national infrastructures and the financial system must be ready for cyber-attacks, attacks that not only disrupt the computer systems but also cause damage in the real world. The right thing to do is to encourage collaboration between the central entities at the financial sector, the government and the

security system. Together with the infrastructure providers, the internet providers and the information security companies, an effective infrastructure can be established to cope with these attacks. Most experts agree that this is the most important lesson from the case of the "Saudi Hacker". Usually, several organizations are attacked together, so it is best they defend themselves together. This is what must be done in order to form a uniform front to the threat raise the level of awareness, share information between organizations, gather intelligence and pass it on to the companies found at the cyber front. It will not be too much to expect and even demand from internet providers, through which all of the traffic going through, to act for the removal of the necessary barriers for sharing information with the attacked entities, and to give the users a cyber space that is clean of threats – to the extent possible. The state should promote suitable and updated regulations, as well as encourage and promote the sharing of information on cyber issues. In this context we return to JP Morgan Chase's Chairman, who said:[54]

> "[T]he CIA, the NSA, the Department of Defense -- they actually know what these attacks are at the border sometimes, and we don't."

[54] Ibid 57.

Spotlight on "Anonymous" and its activity in the Middle East and against Israel[55]

"Anonymous" – online and physical activism

"Anonymous" is not an organization or a movement, it cannot be joined, it has no charter or membership fees, it has no leadership or even a set ideology, it is a collection of people sharing a joint objective who come together for a short period of time in matters pertaining to individual freedom and freedom of expression, physical and online, and the prevention of censorship over the internet and governmental restrictions on this medium.[56] All this is by virtue of social responsibility as agents of change in the various countries through propaganda campaigns and online attacks against government websites and information systems and those of various organizations. This activity takes place for the most part in close cooperation with protest agents across the Middle East, creating a certain demographic change among the members, who until the 2011 protests in the Middle East were mainly from North America, Europe and Australia.

The following excerpt testified to the nature of the conduct:[57]

> Anonymous and Telecomix operate in the open; you just need to know where to look. Remember, these groups operate as voluntary do-ocracies. No one is going to tell you what to do or give you orders. Instead, join IRC or the forums and if something strikes your fancy, help out. Once you've been around long enough to get a sense of what's appropriate, start your own project (called an "op"); find some collaborators and get doing. Yup, it's really that simple.

---

[55] The article was written by Tal Pavel tal@middleeasternet.com, a PhD. For the Middle East, CEO of the Middleeasternet Company for research of the internet and the online threats at the Middle East and the Islamic world and lecturer at the School of Communications at the Academic College in Netanya.

[56] Jana Herwig, "Anonymous: peering behind the mask", Gaurdian.co.uk, May 11, 2011. http://www.guardian.co.uk/technology/2011/may/11/anonymous-behind-the-mask

[57] Peter Fein, "Hacking for Freedom", I Wear Pants, March 18, 2011. http://blog.wearpants.org/hacking-for-freedom

This activity is generally channeled into two fields:

- On the one hand, affording the possibility for the residents of the Middle East to create free communication[58] and reach information that has been banned by the authorities. Inter alia, by creating mechanisms that circumvents the various government restrictions on the internet. "Anonymous" uses the internet and mainly the social networks (with an emphasis on Facebook, Twitter) as well as IRC to communicate between individuals, who come from all countries, professions and races.[59]

- On the other hand, to punish the authorities for the restrictions imposed on the freedom of information (with an emphasis on online information) in their countries. In its activity, "Anonymous" does not encourage violence or physical harm but rather supports the changes going on, inter alia, in the Middle East and to help the demonstrators, and on the other hand attack government websites. This is by hacking into a variety of government websites as well as various information systems and stealing data, as a counter action. Every such action is called an Operation and it includes preliminary activity, in most cases with early warning as to the punishment that will be imposed on these governments, as well as preparing a poster suited to the operation.[60]

  Anonops conducts DDOS (we prefer "digital sit-in"), spams fax machines, defaces websites, writes propaganda and otherwise causes a ruckus. There is a wide variety of activities that take place, not all of them legal, and not all of them destructive. Make sure you understand what you're doing before getting involved with ops.

The internet contains instructional material on behalf of its operatives regarding online and physical protest, alongside issues in security and even that of demonstrators in the streets,[61] including large compressed files containing various instructional topics. Many

---

[58] Anonymousworldwar3, "ANONYMOUS – OPERATION MESH – A Press Release", YouTube, February 7, 2011.
http://www.youtube.com/watch?v=kc-JHT0gNtk

[59] mmxanonymous, "HOW TO JOIN ANONYMOUS – A BEGINNER'S GUIDE mobile,", YouTube, December 15, 2010.
http://www.youtube.com/watch?v=XQk14FLDPZg&NR=1 (Accessed on 25 April 2012)

[60] Peter Fein, "Hacking for Freedom,", I Wear Pants, March 18, 2011.
http://blog.wearpants.org/hacking-for-freedom

[61] A 32MB compressed file containing various instructional files in topics such as first aid, secured online publication, a guide for the protestor and more.
NewCarePackLight.zip, mediafire.com
http://www.mediafire.com/?sl6r8tj0raz6aj7
Anonymii, "Anonymous – the ber-secret handbook,", Version 0.2.0, February 20, 2011.
http://www.pdf-archive.com/2011/02/20/sikrit0-2-0/sikrit0-2-0.pdf

video clips containing statements made by the organization can be found on YouTube and on the dedicated channels identified with its activity.[62]

Due to the nature of "Anonymous", the identity of the people behind every activity cannot be determined, nor can their objectives, which naturally are not uniform. It is possible that the initiative for the various operations does not come from "Anonymous" operatives or the notice on the operations blog and certainly not the activity on Facebook, but rather comes from entities attempting to exploit "Anonymous'" activity and its name for their ends. For example, Palestinians have attempted to exploit the rising wave of "Anonymous'" activity for the promotion of their objectives, and Turkish hackers wear virtual covers of this popular interface.

"Anonymous" activity in the Middle East against Israel

"Anonymous'" activity has been articulated in the Middle East in recent years, both in the "Arab Spring" and against Israel. In this review we will examine "Anonymous'" activity against Israel.

As stated, "Anonymous" is not an organization or a movement, but rather a "collection of people" and an "internet phenomenon", in which internet users from around the world take part, with a variety of objectives and ideas, even if contradicting, without an actual agenda. If it were possible to create a core representation of this phenomenon, its underlying ideas are the protection of freedom of expression in the physical world and online; alongside anti-globalism, etc.

The activity against Israel is in not particularly lively and is characterized on the one hand by individual actions which seem attributable to these entities. This, compared with amateur (and also single) attempts to generate actions that appear on the face of things

[62] anonypressreleases, YouTube, March 22, 2011.
http://www.youtube.com/user/anonypressreleases
LetterFromAnon, "A Letter From Anonymous.,", YouTube, December 9, 2010.
http://www.youtube.com/user/LetterFromAnon
ANONPressRelease, YouTube, February 9, 2008.
http://www.youtube.com/user/ANONPressRelease
AnomymousFrancophone, "Anonymous Video,", YouTube, January 26, 2011.
http://www.youtube.com/user/AnonymousFrancophone
AnonymousPanacea, "Anonymous Mirror Channel,", YouTube, December 15, 2010.
http://www.youtube.com/user/AnonymousPanacea
MessengerOfAnonymous, "Hello Church of Scientology,", YouTube, May 29, 2009.
http://www.youtube.com/user/MessengerOfAnonymous
The AnonymousIran,", Anonymous Iran,", YouTube, August 2, 2009.
http://www.youtube.com/user/TheAnonymousIran

to not necessarily be connected to "Anonymous", but that are an attempt to wear the mask and virtual aura of this phenomenon.

In this framework, individual attempts are made to initiate online attacks on Israeli government sites with quality and visibility, in protest of Israel's policies. The most publicized action by "Anonymous" was an attempt of an online attack on the Knesset website on July 28, 2011.

In the framework of this activity, instructions were given as to the date of the online attack on the Knesset website:

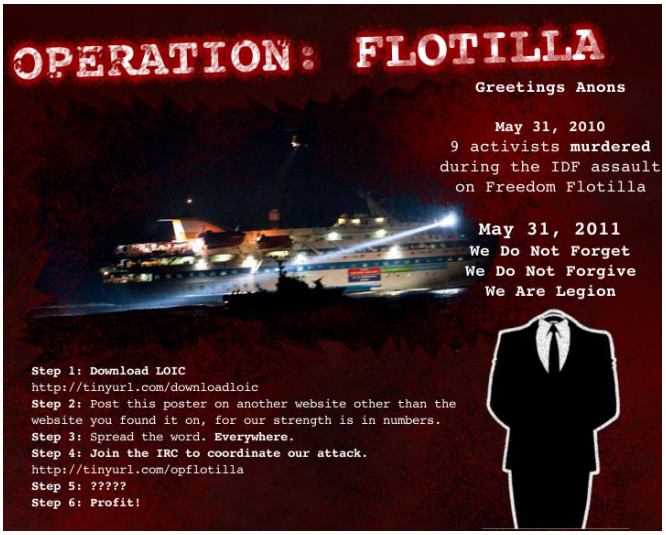
The reference to the website address from where the attack toolkit can be downloaded:

Alongside technical data on the target site (in this case the GoIsrael.com touristic initiative):

And guidelines for action:

These actions of online attacks against Israeli websites are perpetrated as part of "Operations" (#op, #Operation) both general and on specific dates:

Such as, the attempt to create online attacks on the anniversary of the "Turkish Flotilla", including explanations regarding the stages of execution:



These operations happen alongside certain activity against Israel on the social networks, with an emphasis on Facebook, bearing the name of "Anonymous".

However, it is important to remember that this activity is generalized and anonymous and due to its nature, amateurs with interests join it; as a type of "hitchhikers" that enjoy the cover, the aura and the media distribution that affords cover under the virtual mask of "Anonymous".

Today, this activity against Israel is marginal, both against government sites as well as against the civil ones and is often perpetrated by amateur interested entities and not by the main activists. However, it is important to be aware of this type of threat, even if today it is marginal and is perpetrated in low quantity and quality for the most part.

ICT Cyber Desk team:

The following experts comprise our research and writing team:

Dr. Eitan Azani, Deputy Executive Director, ICT

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

Michael Barak (PhD candidate), Team Research Manager, ICT

Shuki Peleg, Information Security and Cyber-Security Consultant

Ram Levi, Cyber-Security Advisor to the National Council for Research and Development

Hila Oved, Special Project Manager, ICT