Cyber-Terrorism Activities

Report No. 4

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

International Institute for Counter-Terrorism (ICT)

Additional ICT resources are available on ICT's website: www.ict.org.il

Highlights

This report covers two main subjets: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse); and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack). The following are among the issues covered in this report:

- Jihadist Web forums highlighted the contribution to the war of attrition against the West of "lone wolf" attackers.
- During the first half of May 2013, visitors to the jihadist Web forum Ansar Al-Mujahideen discussed the leaking of the spyware program Prism by CIA agent Edward Snowden.
- A senior leader of Al-Qaeda proffered personal security advice to those planning to join jihad.
- The Syrian Electronic Army stated that it had attacked other enemies of Syria, among those attacks they hacked few times into Viber, Israeli application for VOIP.
- On July 23, 2013, the Cyber Warriors of Izz al-Din al-Qassam announced their intention of embarking on Stage 4 of Operation Anabil against the US banking system.
- The Cyber-Desk Team extensively reviews development in Cyber Crime using hybrid attack to steel money and the joint effort to contain the threats with cooperation between Government agencies and huge corporates like Microsoft.
- The Iranian's Hacking groups involvement in the cyber space - general reviews
- On May, the US Department of the Treasury designated Liberty Reserve (LR) as a financial institution engaged in money laundering. Liberty Reserve was accused of laundering some $6 billion for clients, among them cyber-criminals engaged in credit card fraud.

Table of Contents

Electronic Jihad 1

Key Topics of Jihadist Discourse, March-July 2013 1

Jihadist Propaganda 4

Defensive Tactics 5

Offensive Tactics 10

Cyber-Crime and Cyber-Terrorism, March-July 2013 16

Unbridled Cyber Crime 16

The Next Plague: Carberp 19

A Combined War on Trojan Horses 20

An Increase in Mobile Phone Malware 21

Case Studies 24

Iranian Hacking Groups 24

Ashiyane 24

Iranian Cyber Army 28

Mortal Combat 29

ITSecTeam 30

Countering Digital Currency 31

Electronic Jihad

Global jihad groups are increasingly venturing into cyberspace. Their use of the Internet for "typical" activities – communication, recruitment of operatives, fundraising, propagandizing, incitement to hatred and violence, intelligence gathering, and psychological warfare – is well-established. In recent years, global jihad and other terrorist organizations have begun to use cyberspace as a battleground for what they call "electronic jihad", attacking the enemy by sabotaging its online infrastructure, using the information available to them from the virtual world to cause mayhem in the real world, and developing their own defensive capabilities against cyber-attack. Following is a selection of recent key acts of electronic jihad, and a brief overview of the key themes reflected in jihadist discourse and propaganda.

Key Topics of Jihadist Discourse, March-July 2013[1]

- Sheikh Ayman al-Zawahiri expressed his support of the mujahideen in various arenas of jihad, and called on Muslims to unite under the banner of monotheism [tawhid] and Islamic law [shari'a]. He threatened France that it would pay a heavy price for its war in Mali.
- The Taliban-Pakistan urged the Pakistani people to learn from the revolutions in Syria and Libya, and embark on a violent revolt against the oppressive Pakistani regime.
- The Islamic Emirate of Afghanistan announced its plan to launch a wave of attacks against coalition forces at the end of April 2013.
- Al-Qaeda in the Arabian Peninsula (AQAP) announced that the ulama' [religious scholars] in Yemen were negotiating a cease-fire between the mujahideen and the Yemeni administration in Sana'a. AQAP's Military Council asked for a stop to Internet requests for guidance and instruction on conducting terrorist attacks, for security reasons.
- A prominent contributor to jihadist Web forums suggested exploiting the current tension between Iran and Saudi Arabia and the events of the Arab Spring to foment popular protests against the Saudi regime.

[1] For a more thorough review of jihadist life on the Web, see the ICT's Jihadi Website Monitoring Group's Periodic reports, at http://www.ict.org.il/ResearchPublications/JihadiWebsitesMonitoring/JWMGPeriodicalReviews/tabid/344/Default.aspx.

- Abu Sufyan al-Azdi Said al-Shihri, a senior member of AQAP, urged the Saudi people to rebel against the Saudi regime and protest the existence of drone bases throughout Saudi Arabia, from which attacks are launched against Muslims in Yemen.
- AQAP Mufti Sheikh Ibrahim al-Rubaysh warned that the Yemeni government's willingness to sign a cease-fire would cost it dearly. He urged Yemeni Army soldiers to defect, because of the continuing and increasing collaboration between Yemen and the US.
- Al-Qaeda in the Islamic Maghreb (AQIM) called on Muslims in North Africa, and especially in Tunisia, to concentrate on implementing Islamic law and fulfilling the commandment of jihad in North Africa only. AQIM urged the French people, and particularly the families of the hostages it was holding, to pressure the French government to withdraw its forces from northern Mali, lest they all bear the harsh consequences.
- Sheikh Abu Ubeyda Yusuf al-Anabi, a senior member of AQIM, lambasted France for its military engagement in Mali. He urged the Muslim Nation to respond to this new Crusader war by attacking French interests worldwide.
- Sheikh Mukhtar bil-Mukhtar, a prominent member of AQIM and leader of the Signers in Blood Brigade, took responsibility for a double terrorist attack in Niger.
- Abu Yahya al-Shanqiti, a member of AQIM's Shari'a Council, called on religious scholars in Mauritania to support the Muslims there by disseminating anti-French propaganda.
- Abu Abd al-Ilah al-Jijli al-Jazaari, the director of the jihadist media center Al-Andalus, which functions under the auspices of AQIM, called on the Ennahda Party, the temporary government of Tunisia, and Tunisia's Minister of the Interior to immediately cease persecuting Ansar Al-Sharia in Tunisia. Bloody clashes between that group and Tunisian security forces were roundly denounced by jihadists and prominent contributors to jihadist Web forums.
- Jaysh Al-Mujahideen wal-Ansar, an Islamist-jihadist umbrella organization in Syria, called for the unification of local jihadist groups and groups of foreign Islamists led by the Chechen Abu 'Umar al-Shishani.
- The Islamic State of Iraq took responsibility for an extensive terrorist attack on March 14, 2013 against the Ministry of Justice – allegedly to avenge the regime's persecution of Sunnis.

- The leader of the Islamic State of Iraq declared the unification of his group and the Al-Nusra Front of Syria, under the name the Islamic State of Iraq and Al-Sham [the Levant]. The leader of the Al-Nusra Front quickly disavowed this unification, and insisted that his group was loyal first and foremost to Al-Qaeda leader Ayman al-Zawahiri.
- Hezbollah's involvement in the Syrian civil war on the side of Bashar al-Assad has led to calls to attack Hezbollah. Recently-established local jihadist groups, such as Ahrar Al-Bekaa, are indeed concentrating on fighting Hezbollah.
- A new Salafi-jihadist group – the Taliban in Al-Sham – declared its establishment and its goal of toppling the Syrian regime.
- Salafi-jihadists in Jordan have stepped up their rhetoric against Hezbollah, and threatened to attack it for of its involvement in the Syrian civil war.
- Visitors to the jihadist Web forum Ansar Al-Mujahideen discussed the possibility of exploiting Israel's border with the Sinai Peninsula to help jihadists slip into Israel disguised as foreign workers.
- Sheikh Mokhtar al-Zubayr, the emir of Somali group Al-Shabab Al-Mujahideen, called on the Somali people to thwart the plans of Ethiopia and Kenya to divide Somalia into areas of influence, and rob the country of its natural resources.
- A member of Al-Shabab Al-Mujahideen counseled Muslims in the US and mujahideen in Somalia to kidnap American citizens, and use them to negotiate for the release of Muslims from US prisons.
- Ansar Al-Muslimeen fi Bilad Al-Sudan announced the "demise" of seven Christians whom it had taken hostage on February 17, 2013, following a failed joint rescue attempt by Great Britain and Nigeria.
- Ahmad Farouq, who is responsible for da'wa [missionary outreach] for Al-Qaeda in Pakistan, exhorted the Bengali people to revolt against the Bangladeshi regime. He complained that Bangladesh's Muslim character was being eroded because of the regime's secularism and pandering its "Western overlords".
- Jihadist Web forums carried lively protests against the regime in Myanmar [Burma], which allegedly discriminates against and oppresses its Muslim residents.
- Jihadist Web forums highlighted the contribution to the war of attrition against the West of "lone wolf" attackers like the Tsarnaev brothers, who placed two bombs at the Boston Marathon; most forum visitors supported this trend.

- A senior leader of Al-Qaeda proffered personal security advice to those planning to join jihad.
- Issues 10 and 11 of the English-language jihadist magazine *Inspire* were published by AQAP, as was a pocket book containing a compendium of optimal targets for the lone wolf attacker. The second issue of *Fursan Al-Balagh* also appeared.
- The fourth issue of *Al-Qaeda Airlines* was published, and was dedicated to making hydrogen cyanide and using it against Western targets.
- AQIM launched a new blog, Muslim Africa, whose goal is to encourage Africa's Muslims to aid jihad.
- A new jihadist magazine, *AZAN,* is being published by the Afghanistan and Pakistan Taliban.

Jihadist Propaganda

The Importance of Jihadist Web Forums to Jihadist Propaganda:

- On April 1, 2013, the jihadist propaganda group Fursan Al-Balagh published an article by Sheikh Abu Sa'ad al-'Amili, a prominent contributor to jihadist Web forums, titled, "Calling on the Mujahideen of Propaganda: Stay Where You Are, Return to Your Villages". In it, al-'Amili expresses support for members of jihadist Web forums who produce propaganda against the enemies of Islam.[2]
- An additional opinion piece by Abu Sa'ad al-'Amili was published on May 15, 2031 on the Al-Fida Web forum, concerning the attempts of the enemies of Islam to take down jihadist Web forums. According to al-'Amili, the forums' renewed online activity proves that the enemy has been defeated. He urged the increase of jihadist propaganda, which is also an arena of jihad against the enemy.[3]

- A visitor to the jihadist Web forum Hanein published a letter in support of the jihadist Web forum Ansar Al-Mujahideen, which had suffered from multiple cyber attacks. The letter stated, "We [at Hanein] see that you are coping with [cyber] attacks like the ones we faced…we hope that our letter will reach you and all of the jihadist forums, and we will make every

[2] http://al-fidaa.com/vb/showthread.php?t=60138
[3] http://al-fidaa.com/vb/showthread.php?t=63661

effort to stand with you, even if we have disagreed [in the past] about one custom or another – for [our] goal is one".[4]

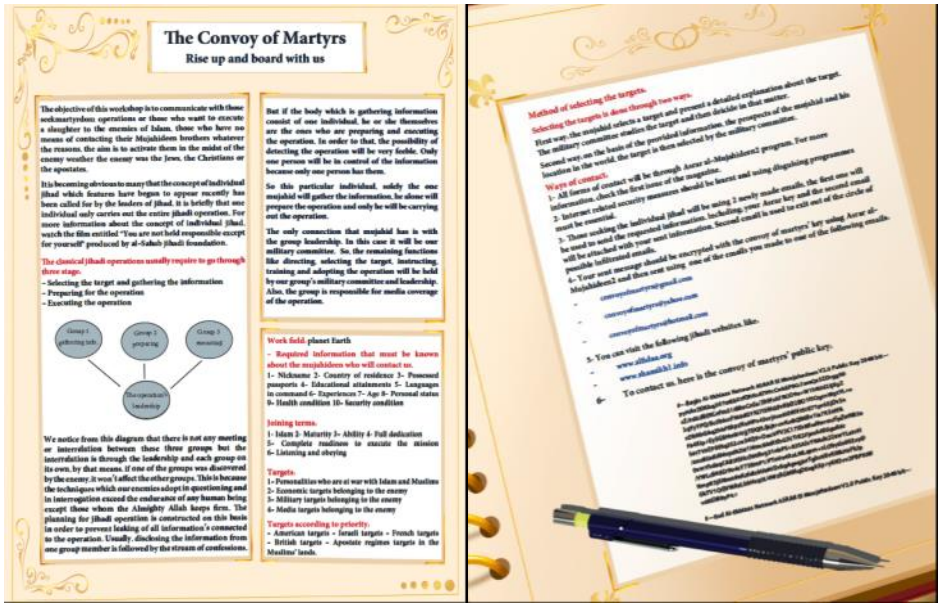
Defensive Tactics

- On March 4, 2013, the Military Council of Al-Qaeda in the Arabian Peninsula (AQAP) published an announcement asking that people cease trying to contact it through the Convoy of Martyrs Project, for security reasons. The following is the announcement, verbatim: "Al-Qaeda in the Arabian Peninsula's military committee announces the ceasing of communication with 'Convoy of Martyrs' via emails and the project's public key. And that is due to security measures. We call upon the brothers who are already in contact to stop the communication".[5] The specifications of the Convoy of Martyrs [Qawafil Al-Shuhada] Project were published in Issue No. 9 of *Inspire*, which appeared in May 2012. The Project was established to recruit Muslims living in Western countries to carry out terrorist attacks in the West. AQIM had invited Muslims with the dedication, faith and willingness to attack Western targets to contact it through Asrar Al-Mujahideen [Secrets of the Mujahideen], a coded message program, in exchange for guidance, instruction, and authorization to hit potential targets.

A banner asking interested parties to stop using the Convoy of Martyrs Project to contact AQAP

[4] http://www.hanein.info/vb/showthread.php?t=317995
[5] http://www.as-ansar.com/vb/showthread.php?t=83002

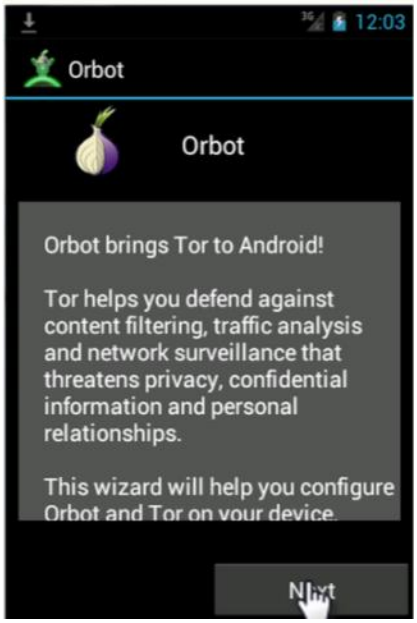
Pages 26-27 of Issue No. 9 of *Inspire* (May 2012) launching the Convoy of Martyrs Project



Pages 28-29 of Issue No. 9 of *Inspire* (May 2012) describing the Convoy of Martyrs Project, and how to use it to contact AQAP

- A visitor to the Ansar Al-Mujahideen Web forum uploaded a program named Orbot, which makes it possible to use the program Tor on an Android platform, along with a detailed explanation of how to use it. He clarified that in order to

safely surf jihadist Web forums using Orbot, it was best to use the browser Orweb or, if that failed, Firefox.[6] Tor is used to surf the Darknet (see below).



Using Orbot on an Android platform

- A news item uploaded to the jihadist Web forum Hanein warned Web surfers against using a VoIP application named Viber, which makes it possible to send instant messages free of charge, including to people in other countries; Viber is owned by an Israeli company. Talmon Marco, the founder of the company, is an Israeli hi-tech executive. Moreover, the company is reputed to save the details of all conversations made using Viber for 30 months, and to allow security and intelligence services to use these data when necessary.[7]

The application Viber, purportedly created and owned by an Israeli company

[6] http://www.as-ansar.com/vb/showthread.php?s=8133c0099e5fe8852e0be4bc1c97c0ac&t=83574
[7] http://www.hanein.info/vb/showthread.php?t=319429

- During the first half of May 2013, visitors to the jihadist Web forum Ansar Al-Mujahideen discussed the leaking of the spyware program Prism by CIA agent Edward Snowden. One thread on the forum contained slides from a visual presentation, which illustrated how much international communications traffic passes through the US – including the responses of communications giants such as Mark Zuckerberg, founder and CEO of Facebook, who claimed he was ignorant of the incident. Although forum members were asked to take special precautions when surfing the Web, one of them saw fit to upload a link to material on the security of the US, including a document chronicling the issuing of security clearance in the US.[8]

The US is a conduit for international cyber-communication

- The general administrator of the Al-Minbar jihadist Web forum officially warned forum members to change their passwords after the forum had been taken down multiple times during the first half of June 2013. The administrator also asked forum members not to let attempts to topple the forum or otherwise interfere with online jihadist activities stop the posts and discussion on the forum.[9]
- During late April 2013, members of the jihadist Web forum Hanein discussed a news item claiming that the Israel Defense Forces (IDF) Intelligence Corps was using the activity of members of Facebook and Twitter to learn about events in the Arab world. In response, one forum visitor called Israel a "terrorist state" that was decimating every last bit of anything good in the world, a state that knows only espionage, murder and destruction.[10]
- A member of the jihadist Web forum Shumukh Al-Islam proposed establishing a special online search engine for the mujahideen, separate from Google and without any connection to the US or the West. Several visitors to the forum

[8] http://www.as-ansar.com/vb/showthread.php?t=91196
[9] http://www.alplatformmedia.com/vb/showthread.php?t=23954
[10] http://www.hanein.info/vb/showthread.php?t=318798

reacted humorously to this suggestion, claiming that it was hardly feasible. In contrast, others praised the suggestion.[11]

An example of what a search engine dedicated to jihad and the mujahideen might look like

- A member of the jihadist Web forum Shumukh Al-Islam drew the attention of forum visitors to the possibility of using an Android-platform mobile phone to take control of an airplane's monitoring systems, and to hijack the airplane. He related that at a security summit held in April 2013 in Amsterdam, a German security expert named Hugo Tesco had reported developing just such a system, which he called Simon; the system contained a malicious code that could attack and infiltrate the security system of an airplane using an Android mobile phone application. Tesco had also revealed that by sending radio waves to the flight management system, it was possible to change the plane's speed and flight path.[12]
- Following multiple difficulties navigating the jihadist Web forum Hanein during April 2013, the forum's administration published an announcement stating that the source of the problems that had paralyzed the forum was a forum member who called himself Gaza al-Khudara', who was asked to cease and desist from his interference and apologize to the forum's visitors. The administration also asked the forum's visitors to focus on a discussion of Islam despite the difficulties of visiting the site, and to behave in accordance with the dictates of Islam. They were also warned lest they get dragged into internal conflict and mutual blame – which only served the enemy.[13]

[11] https://shamikh1.info/vb/showthread.php?t=204033
[12] https://shamikh1.info/vb/showthread.php?t=199519
[13] http://www.hanein.info/vb/showthread.php?t=318670

Offensive Tactics

Attacks on Jewish and Israeli targets:

- On March 2, 2013, a group of hackers calling itself Moroccan Ghosts announced on its Facebook page that it was responsible for hacking into the Web site of the Zionist Federation of New Zealand at http://wwwzfnz.org.nz.[14]

The Web site of the Zionist Federation of New Zealand

- On March 13, 2013, Kalachnikov, a group of Tunisian hackers who ascribe to the idea of global jihad, and The Lawbreakers, another group of hackers, launched an event on a Facebook page – Storm Attack III – to coordinate an attack on Israeli porn sites on April 7, 2013.[15]

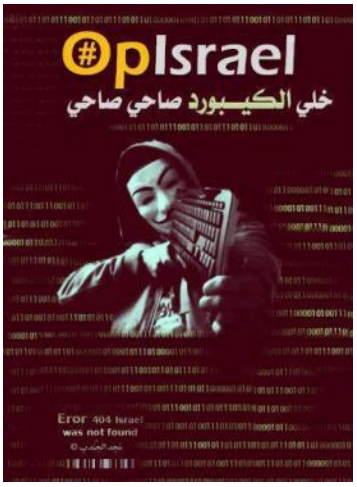
- On March 24, 2013, one of the supervisors of the jihadist Web forum Shumukh Al-Islam published a list of 30,000 employees of Israel's Mossad, Defense Forces and Police Force, as a "bank of targets" for assassination. The list, which could be downloaded in two Excel files, included names, email addresses, residential addresses and telephone numbers. An examination of the "leaked" data indicated that a large number of them were inexact, suggesting that they may have been

[14] https://www.facebook.com/photo.php?fbid=500264296675997&set=a.459080650794362.96563.457696610932766&type=1&theater

[15] https://www.facebook.com/events/344731812304081

stolen from a different site.[16] The list was compiled with the help of a Turkish group of hackers calling itself The Red Hack (Kızıl Hackerlar), and of the infamous hacking group Anonymous.[17]

- The Red Hack was designated as a terrorist group by the Turkish government in July 2012 after it attacked a series of Turkish Internet sites[18] and leaked information from them, such as the identity of foreign diplomats serving in Turkey. The Red Hack has cooperated for several years with Anonymous; the two occasionally commit joint cyber attacks.[19]



The attack was apparently meant to be part of a planned and organized attack by these groups, slated to begin on April 7, 2013, to take down Israeli Internet sites as a sign of solidarity with the Palestinians. This virtual attack campaign was named OpIsrael. Some of the hackers had already begun attacking Israeli sites, without waiting for the chosen date.

[16] http://www.middleeast-internet-monitor.com/?p=3063
[17] https://shamikh1.info/vb/showthread.php?t=195920
[18] For example, an attack on the Web site of the Turkish Police in February 2012: http://gundem.milliyet.com.tr/kizil-hackerlar-polis-sistemini-hackledi/gundem/gundemdetay/27.02.2012/1508505/default.htm
[19] In March 2013, for example, the two groups jointly hacked into the Web site of the Ankara municipality: http://www.sendika.org/2013/03/melih-gokceke-bir-hack-de-anonymoustan

The logo representing the joined forces of Anonymous and the Turkish group The Red Hack (left), and the logo of the Red Hack (right)

- The Tunisian hackers' group Al-Falaja, which propounds global jihad, took responsibility for a series of attacks on Israeli sites and servers during April 2013, as part of the OpIsrael April 7 onslaught. This included an alleged attack on the Web site of the Bank of Israel (http://bankisrael.cov.il), which did not actually occur.[20] Al-Falaja promised to cooperate with Anonymous's extensive online OpIsrael onslaught, in an effort "to remove all Israeli sites from the Internet".[21] In this context, the jihadist Web forum Shumukh Al-Islam published a long list of Israeli sites that had supposedly been hacked into as part of OpIsrael.[22] After Anonymous attacked Israeli Web sites with the aim of eliminating the "Zionist entity" from the Internet, it declared its intention of taking down Web sites associated with Qatar. It also declared its intention of attacking a Jordanian government Web site in retaliation for the arrest of several of its members.[23]
- In June 2013, Al-Falaja took responsibility for hacking into more than 1,000 Israeli Internet sites, mostly of small businesses.[24]

A banner trumpeting Al-Falaja's success hacking into Israeli Web sites

[20] https://www.facebook.com/falagatunisien
[21] https://www.facebook.com/FELLAGATUNISIE
[22] https://shamikh1.info/vb/showthread.php?t=197138
[23] http://www.hanein.info/vb/showthread.php?t=318617
[24] https://www,facebook.com.falaga.ariana

- On July 23, 2013, the so-called Syrian Electronic Army announced that it had hacked into the support page of the application Viber, which facilitates VoIP conversation. The Syrian Electronic Army published a screen shot showing the contact information for people who had accessed the support portal, as well as of the administrators of the portal. Three days later, the Syrian Electronic Army published the access details of the organizational electronic mail server of the founder and information systems administrator of Viber. Two days after that, the Syrian Electronic Army announced that it had succeeded in hacking into the message products page of the AppStore and planting slogans denouncing Apple there. The Syrian Electronic Army also stated that it had attacked other enemies of Syria. In early 2013 it announced that it had hacked into the server of the Turkish Prime Minister's office, and publishing a list of 67 passwords and email addresses culled from that office's site. Two days later, the group claimed that its members had succeeded in hacking into the sites of the Turkish Ministry of the Interior and five other government Web sites. In recent months, the Syrian Electronic Army focused its activities on Western and Saudi Arabian sites, among them Western media sources, whose Twitter accounts it hacked. For example, the group hacked into the Twitter and Facebook accounts of Britain's ITV, *Financial Times* and *The Telegraph*. It also announced it had defaced the application page of Sky News on Google Play, and that it had hacked into the electronic mail server of the Saudi Arabian Ministry of Defense in May 2013.

Attacks on US targets:

- On July 23, 2013, the Cyber Warriors of Izz al-Din al-Qassam announced their intention of embarking on Stage 4 of Operation Anabil against the US banking system. The operation began in 2012, and its third stage was carried out during March 2013. The group claimed that its actions were revenge for the movie "Innocence of Muslims", which was still available on YouTube. It also claimed that as long as the movie was available for viewing, it would continue its attacks.[25] A

[25] For a report on Operation Anabil and its potential damage, see the ICT Cyber Desk's Report No. 2: http://www.ict.org.il/ResearchPublications/ICTCyberDeskReview/tabid/492/Articlsid/1172/currentpage/1/Default.aspx

visitor to the jihadist Web forum Hanein commented that the hackers were Iranian.[26]

- Anonymous and the Tunisian hackers' group Al-Falaja took responsibility for a series of attacks on US government Web sites on April 25, 2013 – purportedly a response to the refusal of the US to free an Algerian hacker named Hamza Bendelladj,[27] who was arrested in Thailand and extradited to the US in January 2013 for stealing money from more than 250 American banks using a computer program he had developed.[28]
- During the latter half of May 2013, visitors to the jihadist Web forum Ansar Al-Mujahideen discussed an additional cyber attack by Anonymous against Guantanamo Prison, where the US incarcerates security prisoners, some of them members of Al-Qaeda. A prison spokesman related that a cyber attack on May 20,2013 had paralyzed the prison's wireless Internet system. Anonymous clarified that the attack had been meant to express support for prisoners who were on a hunger strike. One visitor to Ansar Al-Mujahideen commented that some members of Anonymous were Muslims from the Arabian Peninsula and North Africa; he hoped that the "Crusader" enemy would taste bitterness of a kind it had never before tasted. Other visitors to the forum praised the work of Anonymous.[29]
- During late May 2013, visitors to the jihadist Web forum Ansar Al-Mujahideen discussed a newspaper article about Israel's preparations for an additional electronic attack by Anonymous, which was scheduled for Saturday, May 25, 2013. One forum visitor noted that although people from many countries – including the US, Canada, Great Britain, Italy and other European countries and the countries of the Arabian Peninsula – were participating in the electronic war on Israel, the most important war was the economic struggle against the

[26] http://www.hanein.info/vb/showthread.php?t=315125
[27] https://www.facebook.com/FELLAGATUNISIE
[28] http://www.bbc.co.uk/news/technology-22432178
[29] http://arabic.rt.com/news/616073-%D8%A7%D9%8A%D9%82%D8%A7%D9%81_%D8%AE%D8%AF%D9%85%D8%A9_%D8%A7%D9%84%D8%A7%D9%86%D8%AA%D8%B1%D9%86%D8%AA_%D8%A7%D9%84%D9%84%D8%A7%D8%B3%D9%84%D9%83%D9%8A_%D9%88%D8%AD%D8%AC%D8%A8_%D8%A7%D9%84%D8%B5%D9%81%D8%AD%D8%A7%D8%AA_%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9_%D8%A8%D8%BA%D9%88%D8%A7%D9%86%D8%AA%D8%A7%D9%86%D8%A7%D9%85%D9%88_%D8%AA%D8%AD%D8%B3%D8%A8%D8%A7_%D9%84%D9%87%D8%AC%D9%88%D9%85_%D8%A7%D9%86%D9%88%D9%86%D9%8A%D9%85%D9%88%D8%B3_/

Crusader enemy. In this context, he suggested waging a cyber attack on the American and Israeli stock exchanges; no such attack took place.[30]

Attacks perpetrated by Anonymous or its affiliates:

- During June 2013, Anonymous appeared to be increasingly active in Syria and Egypt. In early June, someone tweeted encouragement to Anonymous to attack the Syrian regime and Hezbollah online, in retaliation for their massacre of the Syrian people. At the end of June, AnonGhost succeeded in hacking into the Web site of the Syrian Ministry of Health and planting messages denouncing the Syrian government and warning it to expect an onslaught by the mujahideen, as "Muslims are everywhere". This same group initiated OpPetrol, an operation that planned a June 20, 2013 attack against 12 countries: the US, Canada, Great Britain, Israel, China, Italy, France, Russia, Germany, Saudi Arabia, Kuwait and Qatar.

  In Egypt, opponents of the new military regime and supporters of deposed President Mohamed Morsi who identified themselves with Anonymous called for a July 30, 2013 cyber attack on the Egyptian government's online presence, by attacking 37 Internet sites and Facebook pages belonging to government offices, press agencies, security forces and banking concerns.

Attacks on Iranian targets:

- Given the increasing tension between Sunnis and Shi'ites, a visitor to the jihadist Web forum Hanein uploaded an announcement that he had hacked into 100 Iranian Internet sites in one day, among them sites for the offspring of short-term "marriages" sanctioned by Shi'ite scholars of Islamic law for the purposes of sexual liaison [mut'ah]. The visitor announced that anyone who wanted to hack into Iranian sites could contact him personally, and he would send them a link that would enable them to take down these sites. He also suggested that hackers threaten to take down certain Facebook pages popular with Shi'ites.[31]

Attacks on Caucasus targets:

- In early April 2013, Caucasus jihadist Web sites were again attacked. However, unlike previous attacks, during this one the sites were not taken off the Internet,

[30] http://www.as-ansar.com/vb/showthread.php?t=90035
[31] http://www.hanein.info/vb/showthread.php?t=318170

but rather the availability of their servers was blocked, such that the sites could not be updated. The only portal that succeeded in posting an announcement was Valiyat Dagestan, which stated that the reason for the blockage was unclear and that the best technical experts were working on resolving the problem.[32]

Cyber-Crime and Cyber-Terrorism, March-July 2013

Recent years have seen increasing cyber attacks on political targets, crucial infrastructure, and the Web sites of commercial corporations. These attacks, which are also, increasingly, receiving international attention, are perpetrated by states (which do not take responsibility for them); groups of hackers (such as Anonymous); criminal organizations; and lone hackers. The following information was culled from the visible (OSINT) and invisible ("dark Web")[33] Internet between March and July 2013.

Unbridled Cyber Crime

Cybernetic crime has caused and continues to cause millions of dollars worth of damage every year. Cyber-crime's potential for profit, at minimal risk, make it very attractive to criminal networks and terrorist organizations. As ever more new actors enter the field and methods become more polished and sophisticated, the difficulty of addressing cyber-crime increases. Systematic cyber-attacks on banking and financial institutions around the world are proving successful and, despite the tendency of banks and financial institutions to keep such information under wraps to guard their stability, some of these successes are being reported in the media. These reports reveal that most cyber-attacks involve the use of credit cards, fraudulent phishing schemes, and the use of Trojan horses; occasionally, more innovative and sophisticated attacks occur. Because it is an international phenomenon, cyber-crime requires a creative approach and both intra-state and international cooperation. Of late, there appears to be a positive trend of cooperation between the business and law enforcement sectors in fighting cyber-crime, as evidenced by Microsoft's struggle

[32] http://vdagestan.com/obyavlenie-o-sajte.djihad

[33] 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.

against botnet networks, which are responsible for some $500 million worth of damage worldwide.[34]

In early May 2013, indictments were handed down in the US against eight persons suspected of involvement in a sophisticated, combined actual-virtual operation that succeeded in stealing $45 million.[35] The suspects attacked twice: On December 12, 2012 they succeeded in stealing $4 million, and on February 19, 2013 they succeeded in stealing some $40 million. Their attack was carried out in three stages:

1. First, they hacked into the computer systems of credit card companies and canceled the credit level of 12 prepaid credit cards; this enabled them to draw money without limitation.
2. Next, they disseminated the prepaid credit cards in 27 countries. It is estimated that several of the prepaid cards, which were associated with the same account, were duplicated.
3. Lastly, during a two-day period, they used the prepaid cards to withdraw cash from some 5,000 ATMs. For example, the cards were used to withdraw more than $2 million in cash from 2,900 ATMs in New York City alone – in the space of only two hours.

This attack was unique because it was perpetrated by both members of a cyber-crime network and ordinary people who simultaneously withdrew cash from ATMs in 27 countries around the world. The attack required a high level of technological prowess, the ability to "think outside the box", and impressive organizational ability.

While such integration between the cyber-world and the real world is apparent in other attacks, as well, the majority of cyber-crimes are committed solely in cyber-space; these involve fraudulent phishing schemes, and the use of spyware and malware to extract the identities of credit card holders or the passwords to bank accounts. Recent attacks reveal a trend of improvement in the techniques and complexity of the malware being used. Cyber-criminals are learning to overcome the obstacles that the financial system is placing before them and to circumvent security systems, for example by sending a text message to the smart phone of a bank

[34] http://www.reuters.com/article/2013/06/06/net-us-citadel-botnet-idUSBRE9541KO20130606?irpc=932
[35] http://www.wired.com/threatlevel/2013/05/eight-charged-in-bank-heist/

client.[36] During March 2013, Symantec published a study analyzing the most prevalent malware in the financial world, as summarized in the following Table:[37]

Table 5

Financial Trojans, including price and other information

Threat	Availability	Maintenance	Price	Distribution	Targeted Institutions	Prevalence
Zeus	Public	Low	Free – $1000s	Low – High	Focused/Broad	High
Spyeye	Public	Low	Free – $700	Low – High	Focused/Broad	Medium
Cridex	Private	Low	N/A	High	Broad	High
Tatanarg	Private	Low	$3000+	Low	Broad	Low
Carberp	Private	Low	$9000+	Low	Broad	Low
Gameover	Custom	High	Priceless	High	Broad	High
Shylock	Custom	High	Priceless	Low	Focused	Low
Bebloh	Custom	High	Priceless	Medium	Focused	Medium

The Table displays eight types of malware, of the Trojan horse variety, and classifies each one according to differing criteria. It should be noted that the malware listed in the Table is free, and does not require any particular technical prowess – two factors that ensure its broad dissemination.

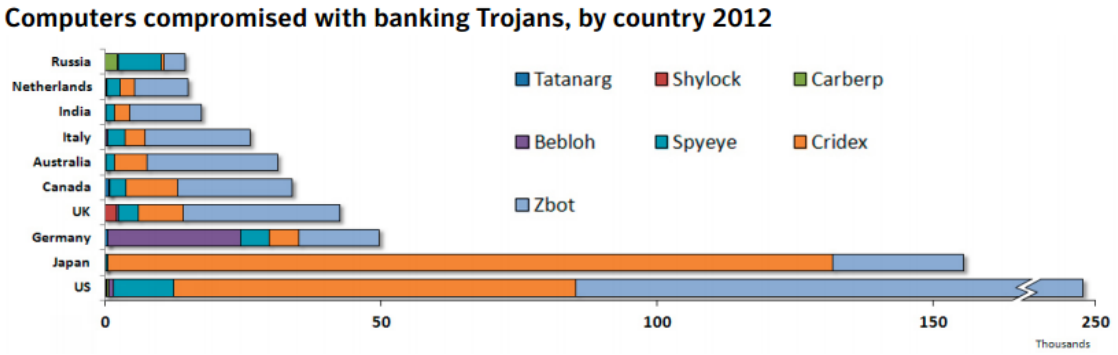
Zeus (also known as Zbot) is a prevalent Trojan horse, which is estimated to have been deployed in over 400,000 computers throughout the world. Several versions of this Trojan horse are extant.[38] Created in 2007, it was first discovered by anti-virus companies in early 2010. The Trojan key Slavik/Monstr (of Russian provenance) sold it over the Internet for several thousand dollars. In 2009, a competing Trojan horse known as Spyeye was developed by Gribodemon and sold on the black marked for less money – about $700. While Trojan horses were proliferating around the world, in 2011 the development code of Zeus was stolen and disseminated over the Internet, enabling developers to make changes in it. This led to a significant increase in the quantity of attacks perpetrated using Zeus. An article by Symantec maps the spread of various versions of Trojan horse in ten countries:[39]

[36] http://www.itu.int/ITU-D/eur/rf/cybersecurity/presentations/ITU_IMPACT_banking_trojans%20by%20Symantec.pdf

[37] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_world_of_financial_trojans.pdf

[38] http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99

[39] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_world_of_financial_trojans.pdf



The Next Plague: Carberp

As can be seen in the data presented by Symantec, the Carberp Trojan horse was prevalent primarily in Russia and Ukraine. Although it was not as broadly disseminated as was Zeus, Carberp is estimated to have caused at least $250 million worth of damage. Carberp malware is very advanced; it costs as much as $40,000 on the black market. In late June 2013, the original code of Carberp was leaked; this may lead to a significant increase in its dissemination, the development of additional versions of Trojan horse based on it, and an increase in attacks around the world.[40]

Carberp uses five different security breaches to infect a targeted computer. The initial "infection" is "spread" through phishing, using email, or else is implanted in an Internet site. Infection involves constructing a Trojan horse in the heart of an operating system and camouflaging it to look like a seamless part of regular operation, so that it is difficult to identify. Once the Trojan horse has been embedded, the targeted computer is linked to a distant command and control (C&C) server; this facilitates both remote control of the computer and updates to the Trojan horse itself, as more progressive versions of it are developed. A C&C server operates through two-way communication with the attacked computer, while another server – a data harvesting server – collects data from the vulnerable computer only. The attacker chooses the type of data he wishes to collect – e.g., account information, passwords, data from browsers that the computer saves – and then uses the data to launch a "man-in-the-browser" attack, which enables the attacker to observer the victim's Internet traffic and interfere with anti-virus efforts.

This particular Trojan horse is sophisticated, and poses a real danger. Because its open code has been leaked, we may see different versions of this Trojan horse in the

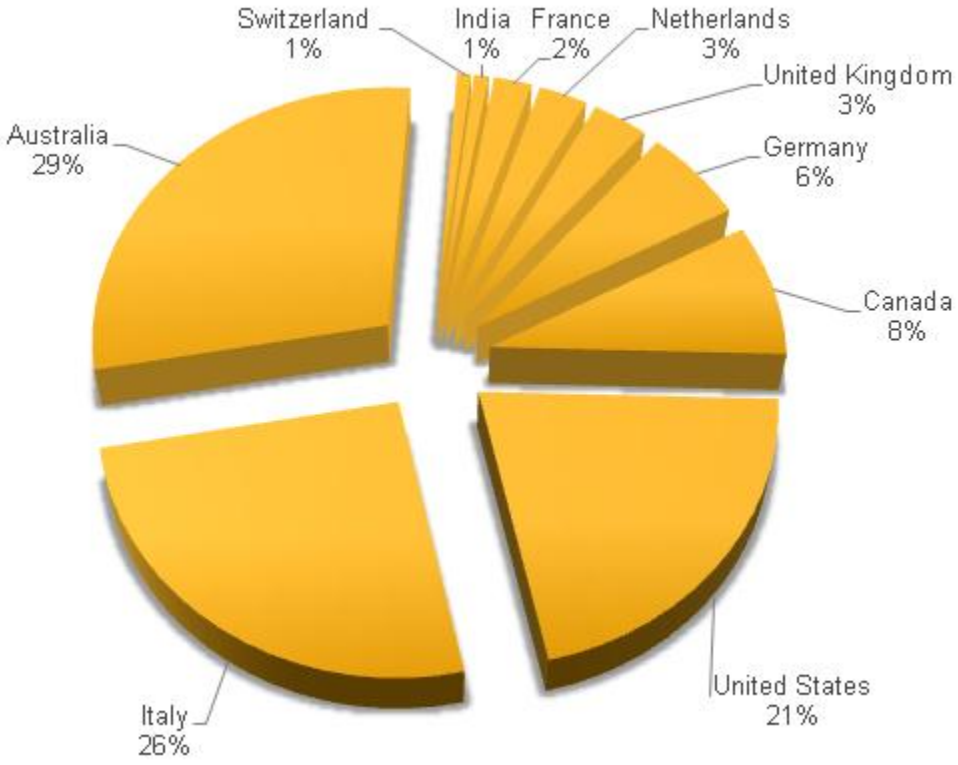
[40] http://www.tripwire.com/state-of-security/vulnerability-management/carberp-botnet-lifecycle-overview-infographic/

near future. The very change in the code itself is liable to make it difficult for anti-virus and other defense systems to identify new versions.

A Combined War on Trojan Horses

As noted, a key component of the Trojan horse is its linkage to the C&C server, which controls the computers that have been infected. Such networks are known as botnets; one of the largest such networks in the world is the Citadel Network. It is estimated that the Citadel Network covers millions of computers worldwide; this botnet was used to steal the details of credit cards and bank accounts from some of these computers. This in turn led to the theft of some $500,000 from private credit and bank accounts around the world.[41] The Citadel Network has apparently also been used in DDoS attacks.[42]

The following pie chart shows the distribution of the Citadel Network as of January 2013:[43]



[41] http://www.reuters.com/article/2013/06/06/net-us-citadel-botnet-idUSBRE9541KO20130606?irpc=932
[42] http://www.mcafee.com/uk/resources/white-papers/wp-citadel-trojan.pdf
[43] http://www.symantec.com/connect/blogs/citadel-s-defenses-breached

At the beginning of June 2013, Microsoft and international law enforcement agencies launched a joint operation – Operation b54 – to paralyze the Citadel Network's C&C servers and thereby "liberate" the infected computers.[44] Microsoft claims to have succeeded in freeing more than 1,400 servers from the Internet,[45] and thereby interfering with the functioning of the Trojan horse in two million computers, in effect "liberating" them from the hidden control of Citadel's C&C servers.

Operation b54 was the first example of cooperation between the business sector (Microsoft) and the public sector (law-enforcement), each of which used its unique tools and skills to fight cyber-crime. No less important is the example this Operation provides of international cooperation, trans-national preparation and support, and the involvement of the FBI, Europol and the multiple CERTs. A Microsoft press release states:

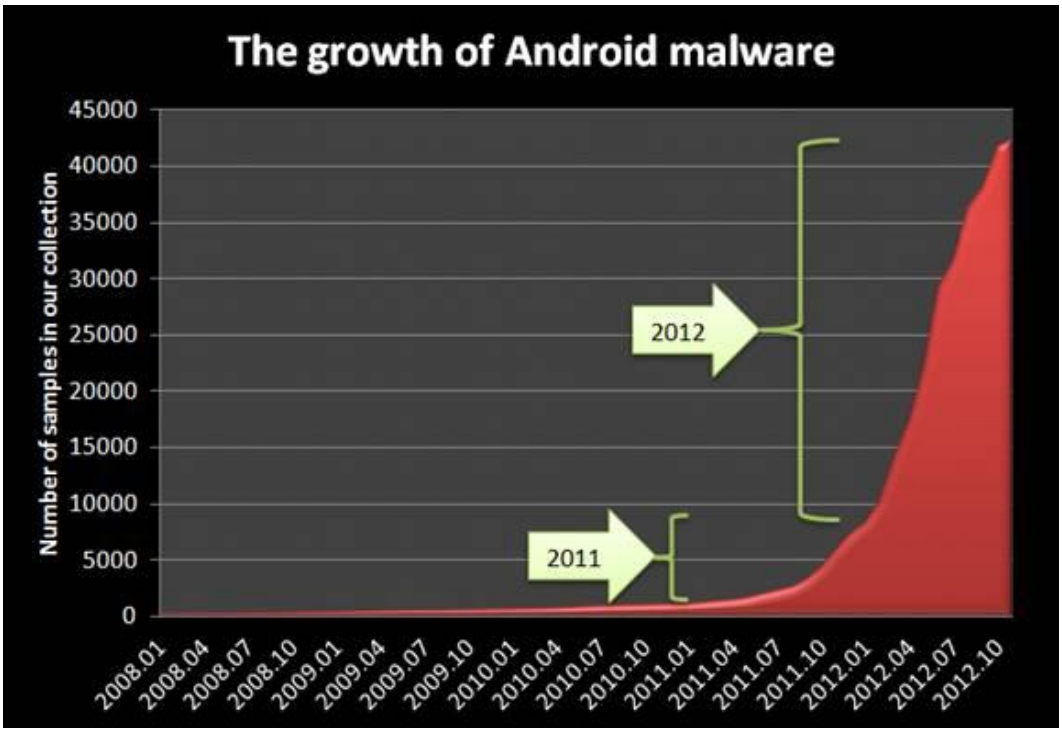
> "This operation serves as a real world example of how public-private partnerships can work effectively within the judicial system, and how 20th century legal precedent and common law principles dating back hundreds of years can be effectively applied toward 21st century cybersecurity issues."[46]

An Increase in Mobile Phone Malware

Mobile telephones are an ideal target of attack. The age of the smart phone has ushered in the perfect spy machine. Mobile phones, especially smart phones, emit GPS signals that can be followed; they can be used to eavesdrop and listen to audio and video content, and they provide access to passwords and files, telephone numbers and email contact lists. The spread of sophisticated mobile phones has piqued the interest of those anxious to exploit security breaches.

A report published by Kaspersky[47] shows a sharp growth in the malware for Android smart phones between 2011 and 2012:

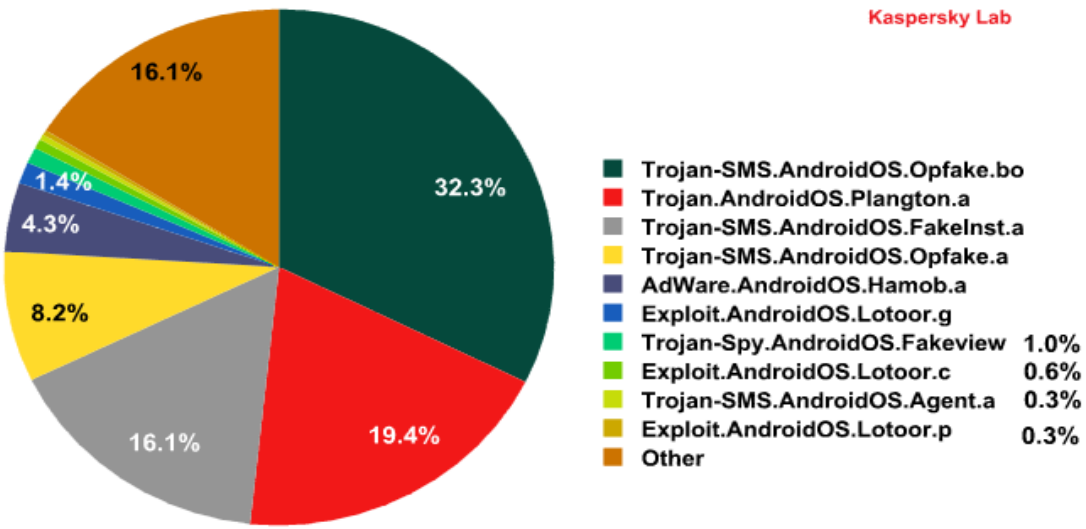
[44] http://www.microsoft.com/en-us/news/Press/2013/Jun13/06-05DCUPR.aspx
[45] http://blogs.technet.com/b/microsoft_blog/archive/2013/06/05/microsoft-works-with-financial-services-industry-leaders-law-enforcement-and-others-to-disrupt-massive-financial-cybercrime-ring.aspx
[46] http://www.microsoft.com/en-us/news/Press/2013/Jun13/06-05DCUPR.aspx
[47] http://www.securelist.com/en/analysis/204792254/Kaspersky_Security_Bulletin_2012_Malware_Evolution



According to an analysis of the spyware developed for cellular telephones,[48] the decisive majority of this spyware has been developed for Android operating systems, which are part of Google. Kaspersky Labs have classified the spyware into the following three groups:

1. SMS Trojans, most of which were deployed in Russia and sent text messages to unwitting paying operators.
2. Plangton, which inserted a malicious code into applications that could be downloaded free, which would both present advertisements and change the browser home page.
3. Lotoor, which includes various types of spyware that exploit access to the heart of the operating system.

[48] http://www.securelist.com/en/analysis/204792283/Mobile_Malware_Evolution_Part_6



As the above pie chart shows, cyber-criminals use about half of all malware to generate profit by sending text messages to recipients who charge an additional fee; since this fee is nominal, most users do not identify the theft. Although such thefts may amount to a few dollars per user per month, when tens of thousands of users are involved, the sum of the theft becomes significant.

In early June 2013,[49] reports were received of a new Trojan horse in the Android system: Backdoor,AndroidOS.Obad.a. This spyware was updated and received instructions from a C&C server. In addition to downloading additional updates and spyware, the C&C server drew files and data from the mobile phones in which the spyware had been embedded to the attackers' server. The spyware also disseminated itself through Bluetooth devices to all of the open mobile phones in its vicinity. According to Kaspersky Labs, the structure and method of this spyware are similar to that of the Windows operating system spyware in their sophistication and use of multiple breaches in security. Clearly, spyware and malware for mobile telephones is improving.

In early July 2013, a critical security breach was identified in the heart of the Android system, affecting 99% of the Android mobile phones in the world (an estimated 900 million mobile phones).[50] This breach enables an attacker to replace legitimate legal programs with malicious ones.

[49] http://www.securelist.com/en/blog/8106/The_most_sophisticated_Android_Trojan

[50] http://www.informationweek.com/security/vulnerabilities/hack-99-of-android-devices-big-vulnerabi/240158013

Android-based devices are not the only ones exposed to danger and breaches. At the Black Hat hackers' conference in August 2013, a group of hackers[51] presented a charger for an Apple device, which included a hardware component that knows how to break into the device in less than one minute. While actual physical access to the mobile device is necessary for hacking, it is nevertheless apparent that public mobile telephone chargers represent another dimension of danger.[52]

Case Studies

Each newsletter issued by the ICT's cyber-desk will discuss in greater detail a recent incident of cyber-attack. This issue highlights groups of hackers from Iran.

Iranian Hacking Groups[53]

Ashiyane

Ashiyane, meaning "nest" in Persian, is one of the most well-known – if not the best known – and one of the oldest groups of hackers in Iran.[54] The group also functions as an information security company (which supports products and provides services and instruction) under the name Ashiyane Security Group.[55] It should be noted that many Iranian hacking groups function as security companies and call themselves "security groups" (in Persian, goruh-e/tim-e (group) amniyati (security)).

Ashiyane was founded in 2003[56] by three people: Behrooz Kamalian (aka Behrooz_Ice), Nima Salehi (aka X7Q), and Ali-Reza Shirazi (aka ActionSpider).[57] Kamalian[58] is clearly the most prominent and renowned member of Ashiyane, both in and outside of Iran. Kamalian was also personally sanctioned by the EU, and was placed on a list of Iranian human rights violators on October 12, 2011[59] because of his ties to the IRGC (he is the only one of the group to be placed on that list). Nima

[51] http://www.blackhat.com/us-13/briefings.html#Lau
[52] https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf
[53] This article was written by Ran Ben Shalom, an ICT Research Intern and BA student at the IDC.
[54] http://www.bachecode.blogfa.com/post-14.aspx, http://tavaana.org/fa/node/1373
[55] http://www.ashiyane.ir
[56] http://www.bachecode.blogfa.com/post-14.aspx
[57] http://hack.pnuab.ac.ir/%D9%86%DB%8C%D9%85%D8%A7-%D8%B5%D8%A7%D9%84%D8%AD%DB%8C
[58] http://tavaana.org/fa/node/1373
[59] http://aminsabeti.net/1390/07/behrouz-kamalian-in-eus-sanction-list

Salehi, who is thought to be one of the managers of Ashiyane,[60] is strongly identified with the group and is its best-known member after Kamalian. Both are Ashiyane's public face,[61] and cooperate in various overt and "legitimate" endeavors, such as lecturing and presenting seminars on hacking and information security[62] and managing the Ashiyane Web site.[63] Ali-Reza Shirazi, as ActionSpider, is involved in destroying other Web sites.

Initially Ashiyane concentrated on publicizing and disseminating professional and instructional materials on hacking, usually on its own Web site, and for free. Subsequently, Ashiyane expanded its activity, and began informing its members and other Iranian Web administrators of security breaches and vulnerabilities, in an effort to improve Internet security in Iran.[64] Some three years after its establishment, Ahiyane began functioning as an IT security company, as noted above.[65]

Ashiyane's official Web site carries varied content. For one, the site hosts a forum with thousands of members, many of whom contribute actively and meaningfully to an exchange of ideas. The site provides news from the world of IT security, and articles by Ashiyane members on a variety of professional topics. On July 9, 2011, the site posted an article indicating that Ashiyane's members had been ranked by the Zone-H.org Web site as being among the "first-rate hackers in the world" (this fact has been cited countless times in reference to the group).[66] The Ashiyane Web site also features announcements about the group's recent operations,[67] including the following: the destruction of the NASA Web site[68] in August 2005;[69] the invasion of

---

[60] http://hack.pnuab.ac.ir/%D9%86%DB%8C%D9%85%D8%A7-%D8%B5%D8%A7%D9%84%D8%AD%DB%8C

[61] https://twitter.com/amirmansoury/statuses/196294513264828417
@farentaghizadeh

[62] http://pichamedpic.blogfa.com/tag/%D8%A8%D9%87%D8%B1%D9%88%D8%B2-%DA%A9%D9%85%D8%A7%D9%84%DB%8C%D8%A7%D9%86-%D9%88-%D9%86%DB%8C%D9%85%D8%A7-%D8%B5%D8%A7%D9%84%D8%AD%DB%8C

[63] http://ashiyane.org/aboutushat

[64] http://www.bachecode.blogfa.com/post-14.aspx, http://tavaana.org/fa/node/1373, http://hack.pnuab.ac.ir/%D9%86%DB%8C%D9%85%D8%A7-%D8%B5%D8%A7%D9%84%D8%AD%DB%8C

[65] http://hack.pnuab.ac.ir/%D8%A2%D8%B4%DB%8C%D8%A7%D9%86%D9%87

[66] http://www.ashiyane.ir/archive.php?id=51

[67] It sometimes seems that Ashiyane targets non-Iranian Web sites; however, Kamalian has admitted that the group does attack Iranian targets, such as sites that defame the Qur'an. Some publications claim that Ashiyane also acts against Iranian institutions such as the Web site of the Assembly of Experts and prominent clerics. See http://tavaana.org/fa/node/1373 and http://bachecode.blogfa.com/post-14.aspx

[68] NASA was a target of other Iranian groups. For example, in May 2012, a group named Cyber Warriors published the Web sitehttp://www.today.com/id/47522497/ns/today-today_tech/t/iranian-cyber-warriors-team-takes-credit-nasa-hack/#.UdVqafmovmh (NASA had attacked the site of Ajax Team: http://ajaxtm.com). In addition, in December 2011, a blog by the head of the group published instructions

1,200 American Web sites[70] in response to the pastor Terry Jones' declaration of his intention to burn copies of the Qur'an on the anniversary of 9/11; the defacement of "hundreds of Israeli and British Web sites"[71] on September 17, 2009m in protest against "Israeli crimes against Palestine";[72] an attack on 100 Israeli Web sites ending in ".il" (including, purportedly, a takedown of the Mossad Web site) on January 7, 2009, in response to Israel's actions in the Gaza Strip.[73] The Ashiyane Web site also logs past activities, including an attack two years ago against 100 Israeli and 500 Danish Web sites in protest against the caricature of the Prophet Muhammad;[74] an attack two years ago against 100 Arab Web sites, in which the term "Arab Gulf" was changed to "Persian Gulf"; attacks on more than 300 Saudi Arabian, UAE and Bahraini Web sites, in response to an attack on Shi'ite Web sites and "sources of imitation" several days prior to that,[75] and the like.[76]

It has often been claimed that Ashiyane's activities, with their overt patriotic-nationalist bent,[77] are orchestrated by the Iranian regime or the Revolutionary Guards (similar claims have made about the Iranian Cyber Army, see below).[78] Some have even claimed that Ashiyane instructs Iranian security forces[79] or is part of the cyber department of the Revolutionary Guards.[80] Others say that proof of the relationship between Ashiyane and the Iranian government lies in the speed with which the group's activities make headlines in the government-backed media, and

---

on how to attack a site located on one of the servers (and to download XML External Entity Injection through NASA).

[69] http://www.ictna.ir/print/045010 ,/http://www.bachecode.blogfa.com/post-14.aspx

[70] According to Kamalian, the sites were located on 30 different servers and were all hacked into within the space of three days, in an operation involving some 20 hackers. See http://khakrizenoor.blogfa.com/8906.aspx, http://bd-baft.ir/index.php?option=com_content&task=view&id=237

[71] For a list of the targets see http://www.zone-h.org/archive/defacer=Ashiyane%20Digital%20Security%20Team

[72] http://www.ashiyane.ir/archive.php?id=44

[73] http://www.ashiyane.ir/archive.php?id=40

[74] In 2005, a Danish newspaper published a caricature of the Prophet Muhammad that incited significant protests across the Muslim world; see http://www.bachecode.blogfa.com/post-14.aspx, http://tavaana.org/fa/node/1373

[75] http://www.ashiyane.ir/archive.php?id=39

[76] The December 2009 attack on Israeli Web sites, including that of the Cameri Theater, is well known. See http://www.netlaw.co.il/it_itemid_11541.html

[77] http://tavaana.org/fa/node/1373

[78] http://www.azadcyber.info/articles/400; http://tavaana.org/fa/node/1373

[79] Kamalian has admitted that Ashiyane provides services to government and military institutions (in its commercial capacity), but denies that it receives instructions regarding its offensive attacks from these institutions; see http://tavaana.org/fa/node/1373

[80] http://www.azadcyber.info/articles/400

the extensive, positive coverage they receive.[81] Ashiyane has denied having ties to the regime, and insists that it is wholly independent. Moreover, it claims that its open dialog with the media proves that it is *not* connected to the Iranian government.[82]

One of 1,000 Western Web sites defaced by Ashiyane on August 28, 2010 to commemorate "War on Terrorism Day"[83] and protest "crimes against humanity by supporters of terrorism, chiefly the US and Great Britain"[84]

Behrooz Kamalian[85]

[81] The claim has also been made that Ashiyane's activities – clear infractions against Iranian cyber-criminal law – are not only neither denounced nor prosecuted, but rather are supported and encouraged. See http://tavaana.org/fa/node/1373

[82] http://tavaana.org/fa/node/1373

[83] "War on Terrorism Day" is commemorated in Iran to mark the deaths of former President Mohammad Ali Raja'i and former Prime Minister Mohammad Javad Bahonar in an explosion on August 30, 1980; Iran blames the Mojahedin Khalq (MKO) for planting the bomb that caused their deaths. The faces of Raja'i and Bahonar were superimposed on Web sites defaced by Ashiyane.

[84] http://tavaana.org/fa/node/1373

[85] https://www.facebook.com/behrooz.kamalian; http://aminsabeti.net/1390/07/behrouz-kamalian-in-eus-sanction-list /http://www.pichamedpic.blogfa.com/cat-15.aspx

Iranian Cyber Army

In recent years, an entity calling itself the "Iranian Cyber Army" has made headlines for defacing Web sites. The Iranian Cyber Army was first mentioned on December 12, 2009, in conjunction with an attack against the Mowj-e Sabz [The Green Voice] Web site.[86] Since then, the Iranian Cyber Army has attacked targets throughout the world, including Twitter accounts[87] in late 2009, the Baidu search engine in January 2010,[88] the Voice of America Web site,[89] and various sites that serve the Iranian opposition.[90] Even though several years have passed since the Iranian Cyber Army first made its appearance in the media, its identity has remained an enigma. Some claim that one man is behind the entity,[91] while others claim that the entity is a group of hackers with ties to the Revolutionary Guard; yet others have claimed that the hackers are Russians.[92] Claims have even been made that, in effect, the members of Ashiyane are behind the Iranian Cyber Army.[93]

Examination of the actions of the Iranian Cyber Army reveals that its attacks are usually a response to the activities of opposition groups within Iran – e.g., the extensive use that Iran's Green Movement made of Twitter to protest the results of the summer 2009 presidential elections. It has therefore often been wagered that the Iranian Cyber Army is acting in the service of the regime, or else is being guided by it. At the same time, reports exist that the Iranian Cyber Army engages in activities of a different tenor, such as an attack on Mohsen Sazgara, who tried to create instructional materials on how to defend against the Iranian Cyber Army;[94] the publication, in November 2011, of the identities of reservists in the Israel Defense Forces infantry;[95] an attack on the Web site of Azerbaijan state television in February 2012;[96] and threats against an Iranian citizen who in April 2012 revealed

---

[86] The site, which became active after the Iranian presidential elections of summer 2009, supported Mir-Hossein Mousavi and Mahdi Karoubi, and was run by reformists outside Iran; see http://www.tabnak.ir/fa/pages/?cid=77449

[87] http://thelede.blogs.nytimes.com/2009/12/18/twitter-hacked-by-iranian-cyber-army/

[88] http://www.tabnak.ir/fa/pages/?cid=80940

[89] http://www.voanews.com/content/iranian-hackers-attack-voa-internet-sites-116678844/172741.html , http://www.terrorism-info.org.il/data/pdf/PDF_11_048_1.pdf

[90] http://www.farsnews.com/newstext.php?nn=8811110874; http://tabnak.ir/fa/pages/?cid=85737 , http://iranbriefing.net/?p=17256

[91] http://www.bachecode.blogfa.com/post-14.aspx

[92] http://www.bachecode.blogfa.com/post-14.aspx

[93] http://tavaana.org/fa/node/1373, https://www.defcon.org/images/defcon-18/dc-18-presentations/Amit/DEFCON-18-Amit-Cyber-Crime.pdf

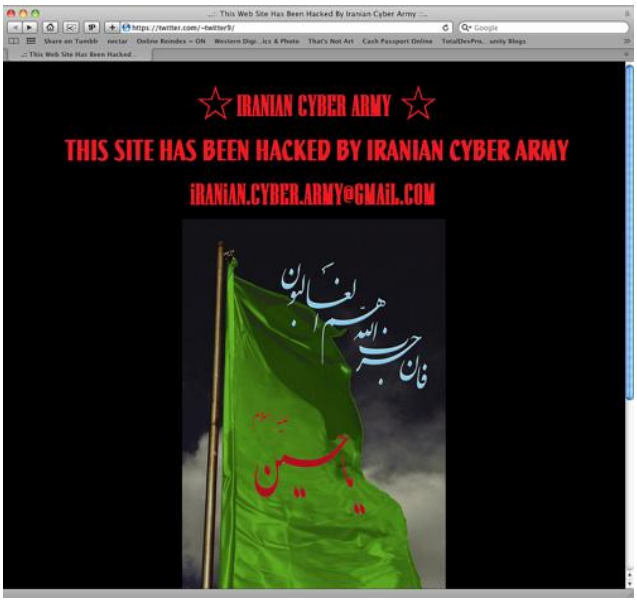
[94] http://www.tabnak.ir/fa/pages/?cid=85501

[95] http://www.israelhayom.co.il/site/newsletter_article.php?id=23770&newsletter=22.11.2012

[96] http://www.bbc.co.uk/persian/iran/2012/02/120223_008-iran-azerbaijan.shtml

the identities of three million bank card holders.[97] In addition, recent reports have claimed that the Iranian Cyber Army established Botnet,[98] or has been involved in cyber-crime.[99]

It is important to stress that much misunderstanding has been generated surrounding the identity of the Iranian Cyber Army. The expression "cyber army" is broadly used by senior Iranian security officials when they discuss establishing defensive and offensive cyber mechanisms for Iran. For example, in March 2011, senior Basij leaders stated that a "cyber army" was functioning as part of the Basij.[100] However, these comments were not referring to any specific entity calling itself the "Iranian Cyber Army".[101]



Defacement of a Twitter account by the so-called Iranian Cyber Army[102]

Mortal Combat

The group **m0rtalkombat**, also known as The Underground Security Team, has also been active in Iran for a number of years. In a relatively unusual step, and unlike most other hacking groups, m0rtalkombat's members do not have ties to the media, refuse to be interviewed, and do not (also) function as an IT security company. The

[97] http://www.terrorism-info.org.il/Data/articles/Art_20324/H_081_12_353850276.pdf
[98] http://www.computerweekly.com/news/1280094205/Iranian-Cyber-Armys-plan-to-sell-botnets-increases-threat-level
[99] http://www.seculert.com/blog/2010/10/iranian-cyber-army-strikes-back.html
http://www.tabnak.ir/fa/pages/?cid=85501
[100] http://www.terrorism-info.org.il/he/articleprint.aspx?id=17938
[101] The Persian Wikipedia entry for "Iranian Cyber Army" is a prime example of this hodgepodge.
[102] http://zahra-hb.com/1388/09/twitter-hacked-by-iranian-cyber-army-group

information available on the Internet about m0rtalkombat is therefore rather limited. At the same time, like other groups, m0rtalkombat maintains a Web site with an active forum, sections of which are cordoned off from the general public. In the past, it has been suggested[103] that this mysterious group[104] was behind the mahdi virus that attacked Israeli targets, as reported in the summer of 2012.[105]

From the Web site of m0rtalkombat[106]

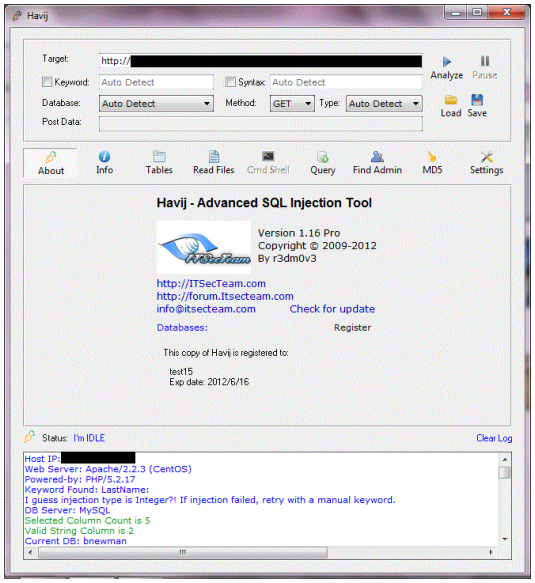
ITSecTeam

Another group worthy of note is ITSecTeam. Like other groups, ITSecTeam has a Web site[107] in its capacity as a legitimate IT security company, known in Persian as Amn Pardazesh Kharazmi.[108] Yet unlike similar companies in Iran and elsewhere, ITSecTeam does not publish any information about its employees on its Web site.[109] Somewhat unusually, relative to other groups, ITSecTeam has earned renown for developing and disseminating hacking tools,[110] the most famous of which is the Havij tool [havij means carrot, in Persian]. Havij is an interface for the automation of SQL injection;[111] it is in very wide use, because it is simpler and more user-friendly than other such tools.[112] ITSecTeam has also produced a Web Application Exploiter – WAppEx – which is used for the pen testing of Windows or Linux Web applications (and, of course, for attacking Web sites). This tool uses Havij for SQL injection.

---

[103] http://www.cybersquared.com/there-is-something-about-mahdi./
[104] http://www.m0rtalkombat.com
[105] http://www.seculert.com/blog/2012/07/mahdi-cyberwar-savior.html
[106] https://www.cybersquared.com/there-is-something-about-mahdi/
[107] http://itsecteam.com./
[108] http://ir.linkedin.com/pub/farshad-shahbazi/69/b11/302
[109] http://itsecteam.com/page/about-us
[110] If used for pen testing, such tools are considered "legitimate hacking tools".
[111] http://isc.sans.edu/diary/The+Havij+SQL+Injection+Tool/11011
[112] http://www.troyhunt.com/2012/10/hacking-is-childs-play-sql-injection.html

Two prominent members of ITSecTeam are Farshad Shahbazi (aka r3dm0v3), who is credited with developing both Havij and WAppEx,[113] and Amin Shokuhi (aka Pejvak).[114] Two additional members of this group are Yashar Shahinzadeh[115] and Behzad Ravanbakhsh.[116]



The Havij tool developed by ITSecTeam[117]

Countering Digital Currency

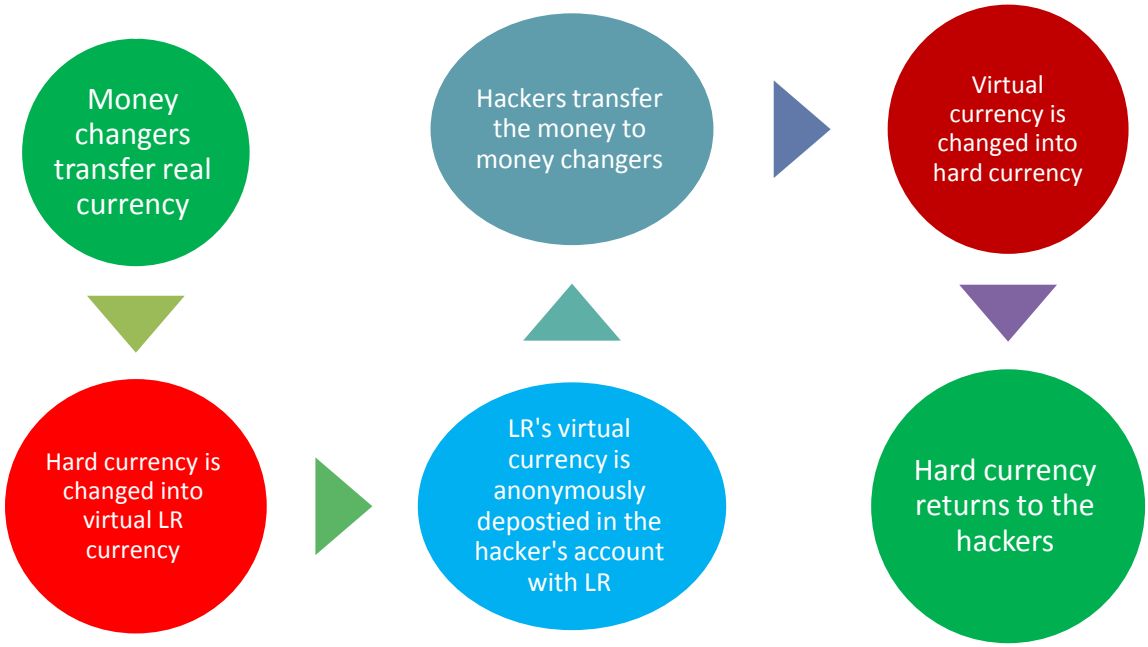
On May 28, the US Department of the Treasury designated Liberty Reserve (LR) as a financial institution engaged in money laundering.[118] Liberty Reserve was accused of laundering some $6 billion for a cadre of clients, among them cyber-criminals engaged in credit card fraud, online pedophilia, and Internet hacking.[119]

Located in Costa Rica, Liberty Reserve is considered "the oldest and most secure virtual payment service in the world";[120] it has used a unique virtual currency that it

[113] http://ir.linkedin.com/pub/farshad-shahbazi/69/b11/302
[114] http://exploitsdownload.com/search/Amin%20Shokohi./
[115] http://ir.linkedin.com/pub/yashar-shahinzadeh/68/60a/aaa
[116] http://ir.linkedin.com/pub/behzad-ravanbakhsh/41/729/233
[117] http://www.google.co.il/imgres?imgurl=http://www.itsecteam.com/sites/default/files/products_images/main0_1.gif&imgrefurl=http://www.itsecteam.com/products/havij-v116-advanced-sql-injection/&h=727&w=666&sz=147&tbnid=POLGwrB9b_EkrM:&tbnh=97&tbnw=89&zoom=1&usg=__nksyRKamj5nqfRLstT562CC0PrE=&docid=k_D6P0VB0VL83M&sa=X&ei=mR2nUfqxGbHZ4QTx7YHgDQ&ved=0CC8Q9QEwAQ&dur=3378
[118] http://www.treasury.gov/press-center/press-releases/Pages/jl1956.aspx
[119] http://online.wsj.com/article/SB10001424127887323855804578511121238052256.html?mod=business_newsreel#project%3DLIBERTY0529%26articleTabs%3Darticle
[120] http://www.bbc.co.uk/news/technology-22680297

developed. Liberty Reserve cooperated with unregulated money changers from Russia, Nigeria and Vietnam. Liberty Reserve changed hard currency into virtual currency and invested it in a virtual account; anonymous transfers could then be made of the virtual currency, without any chance of their being monitored or identified. Liberty Reserve charged a 1% fee for every transfer of hard currency into virtual currency. Liberty Reserve helped clients transfer money anonymously, without having to identify themselves, and without fear of oversight from law enforcement or regulatory agencies. This system became very popular among hackers and black-market traders, who used it to transfer money back and forth "safely".

The following flow chart illustrates how Liberty Reserve worked:



As can be seen in the flow chart, Liberty Reserve did not engage in "classic" money laundering involving the purchase and sale of goods. Rather, it created a system for transferring monies that obviates surveillance or monitoring. The US Department of the Treasury sees Liberty Reserve as a danger – both as a money launderer and as a financer of terrorism.[121]

[121] http://www.fincen.gov/statutes_regs/files/311--LR-NoticeofFinding-Final.pdf

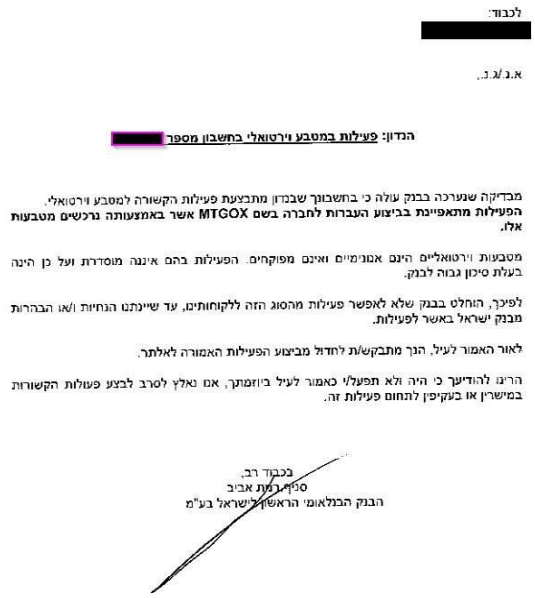
Liberty Reserve marks a precedent. The US government may use the authority granted it by the Patriot Act to halt Liberty Reserve's activity, raising fears of similar future actions against virtual currency such as Bitcoin.[122]

Bitcoin is one of the better-known virtual currencies in the world; it recently became a product for investment, making headlines in the financial press. Bitcoin was first introduced in 2008 by Satoshi Nakamoto (later understood to be a pseudonym), who proposed a new conceptualization of virtual currency based on an algorithm and involving a process of "minting". Minting is on the wane; it is estimated that the total number of Bitcoins will amount to 21 million units. Minting requires advanced processing ability, such that no one single computer cannot accomplish it – except in a peer-to-peer process. Today it is possible to purchase Bitcoin "minting machines", which are capable of making swift calculations. For more information, see www.butterflylabs.com.

Bitcoin has been examined by the Central Bank of Europe, which determined that it was necessary to monitor Bitcoin's development in the world market, so as to divine its influence on the actual market.[123]

In early June, The Beinlumi [International] Bank (a consortium of three Israeli banks) refused to authorize a bank transfer for Mt.Gox, the leading Web site for buying and selling Bitcoin. The consortium's decision was a private initiative, independent of any instruction by the Bank of Israel, and was reached because of the risk of money laundering and terrorism financing.[124]

[122] http://www.forbes.com/sites/petercohan/2013/05/29/after-liberty-reserve-shut-down-is-bitcoin-next/
[123] http://www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf
[124] http://www.holesinthenet.co.il/holesinthenet-media-story-2520



לכבוד:
[redacted]

א.נ./ג.נ.,

הנדון: **פעילות במטבע וירטואלי, בחשבון מספר** [redacted]

מבדיקה שנערכה בבנק עולה כי בחשבונך שבנדון מתבצעת פעילות הקשורה למטבע וירטואלי.
הפעילות מתאפיינת בביצוע העברות לחברה בשם MTGOX אשר באמצעותה נרכשים מטבעות אלו.

מטבעות וירטואליים הינם אנונימיים ואינם מפוקחים. הפעילות בהם איננה מוסדרת ועל כן הינה בעלת סיכון גבוה לבנק.

לפיכך, הוחלט בבנק שלא לאפשר פעילות מהסוג הזה ללקוחותיו, עד שיינתנו הנחיות ו/או הבהרות מבנק ישראל באשר לפעילות.

לאור האמור לעיל, הנך **מתבקש/ת** לחדול מביצוע הפעילות האמורה לאלתר.

הרינו להודיעך כי היה ולא **תפעל/י** כאמור לעיל ביוזמתך, אנו נאלץ לסרב לבצע פעולות הקשורות במישרין או בעקיפין להנחם פעילות זה.

בכבוד רב,
ספיר רמות אביב
הבנק הבינלאומי הראשון לישראל בע"מ

A letter from the Beinleumi Bank informing a client it would not accept Bitcoin

Although anonymity is a fundamental principle of Bitcoin, Mt.Gox instituted a policy of identification for its users, in an attempt to monitor buyers and sellers;[125] it defined three client groups differing withdrawal limitations.[126] Regular clients were limited to withdrawing up to $1,000 per day; verified status level 1 clients were limited to withdrawing up to $10,000 per day, to a monthly limit of $50,000; and verified status level 2 clients were limited to a daily withdrawal of up to $100,000, to a monthly limit of $500,000. Although other such Web sites exist, the Mt.Gox Web site is the leader in the sale of currency. Mt.Gox also allows for the transfer of currency directly between users, without a middleman.

A study published in May 2012[127] examined the anonymity of Bitcoin, in light of the perception that transfers and trade in this currency could be monitored. The study found that Bitcoin is not subject to a central authority or regulator, and therefore no institution monitors its activity. On the other hand, the history of deals and transfers in Bitcoin are public. The study concludes that Bitcoin should be used with caution, and not transferred to entities with which one does not wish to be identified.

[125] https://mtgox.com/press_release_20130530.html
[126] https://mtgox.com/press_release_20130313.html
[127] http://arxiv.org/pdf/1107.4524v2.pdf

Bitcoin is a renowned virtual currency, but it is not the only virtual currency.[128] Other such currencies include Namecoin, Litecoin and PPcoin. Virtual currencies are increasing exponentially: By mid-2013 there were three times as many types of virtual currency extant as there had been at the beginning of 2013. In the virtual world as in the real world, it is reasonably likely that a number of key currencies will be for sale. As long as government agency is involved in the dealings in virtual currencies, a fear of money laundering and terrorism financing will persist.

Timeline of Cryptocurrencies and Various Forks/Clones[129]

Name	Symbol	Release	Author	Innovations
1. bitcoin	BTC	2009/01	satoshi	Decentralized ledger currency
2. namecoin	NMC	2011/04	vinced	Decentralized dns
3. multicoin		2011/06	sacarlson	
4. devcoin	DVC	2011/08	Unthinkingbit	
5. ixcoin	IXC	2011/08	Nasakioto	
6. solidcoin	SC	2011/08	CoinHunter	
7. geist geld	GG	2011/09	Lolcust	
8. tenebrix	TBX	2011/09	ArtForz, Lolcust	Scrypt proof-of-work
9. rucoin	RUC	2011/10		
10. fairbrix	FBX	2011/10	coblee	
11. litecoin	LTC	2011/10	coblee	
12. coiledcoin	CLC	2012/01	makomk	
13. liquidcoin	LQC	2012/01	Nicksasa	
14. timekoin		2012/06	knightmb	
15. bbqcoin		2012/07	Cubox	
16. ppcoin	PPC	2012/08	Sunny King	Proof-of-stake
17. qubic		2012/09		Come-from-Beyond
18. terracoin	TRC	2012/10		
19 freicoin	FRC	2012/12	maaku, jtimon	
20. ripple	XRP	2013/01	jed/OpenCoin	
21. novacoin	NVC	2013/02	Balthazar	
22. bytecoin	BTE	2013/04	bryanmills	
23. mincoin	MNC	2013/04		
24. feathercoin	FTC	2013/04	bushstar	
25. smallchange		2013/04	lightenup	
26. chncoin	CNC	2013/05		
27. bitbar	BTB	2013/05		
28. yacoin	YAC	2013/05	pocopoco	
29. royalcoin	RYC	2013/05		
30. franko	FRK	2013/05	defaced	
31. gamecoin		2013/05		
32. powercoin		2013/05	NWO	
33. elacoin	ELC	2013/05	Milkshake	
34. worldcoin	WDC	2013/05		

[128] https://bitcointalk.org/index.php?topic=134179.0
[129] https://github.com/ppcoin/ppcoin/wiki/History-of-cryptocurrency

35. gldcoin	GLD	2013/05		
36. doubloons	DBL	2013/05	shakezula	
37. sunrisecoin		2013/05	JohnDorien	
38. supercoin		2013/05		
39. bitgem		2013/05	mineral	
40. digitalcoin	DGC	2013/05	baritus	
41. nibble	NBL	2013/05	hyoshi	
42. phenixcoin	PXC	2013/05	JohnCar	
43. luckycoin	LKY	2013/05		
44. uscoin		2013/05		
45. dragoncoin		2013/05	zhaojundong	
46. memecoin	MEM	2013/05	muddafudda	
47. hypercoin	HYC	2013/05	zacho56	
48. americancoin	AMC	2013/05		
49. ezcoin		2013/05		
50. fastcoin	FST	2013/05		
51. megacoin	MEC	2013/05	kimoto	
52. infinitecoin		2013/06	fisheater	
53. anoncoin		2013/06	meeh	
54. stablecoin		2013/06	artos	
55. realcoin		2013/06	dolfcao	
56. noirbits		2013/06	barwizi	
57. zenithcoin		2013/06	solracx	
58. argentum		2013/06	AlphaC	
59. onecoin		2013/06	cre8r	
60. emerald		2013/06	picasso	

ICT Cyber-Desk Team

Dr. Eitan Azani, Deputy Executive Director, ICT

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

Shuki Peleg, Information Security and Cyber-Security Consultant

Ram Levi, Cyber-Security Advisor to the National Council for Research and Development and Senior Researcher at Tel Aviv University

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

Nir Tordjman, Cyber Threats Researcher, ICT

Hila Oved, Special Project Manager, ICT