
## Foreword

Cyberspace has become an important battlefield, and an integral part of current and future conflicts. 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 nation-state actors (which do not take responsibility for them); groups of hackers (such as Anonymous); criminal organizations; and lone hackers. Nation-state actors are becoming ever more aware of the cyber threat, and are assessing its effect on their national security. To this end, many of them are finding (and funding) ways to develop the defense mechanisms to cope with the threat, as well as their own offensive capabilities.

Terrorist organizations are also a part of this dynamic, mutable environment. During the past two years, global jihad groups have also been honing their ability to act in cyberspace. They are extending their activities from "typical" use of the Internet for communication, recruitment of operatives, fundraising, propagandizing, incitement to hatred and violence, intelligence gathering, and psychological warfare, to attacks on the enemy's critical infrastructure cyber warfare techiniques. Increasingly, terrorist organizations are integrating the information available to them from the virtual world with that available to them in the real world, and using the former to develop offensive capabilities in the latter. This they call "electronic jihad".

**Given these developments, and as part our belief that "sharing information increases our ability to confront terrorism", the International Center for Counter-Terrorism (ICT) of the Interdisciplinary Center (IDC), Herzliya has decided to disseminate a periodic report and analysis of information gathered by our cyber-terrorism desk.**

This new publication joins the ICT's series of publications:

- A bi-monthly report of the Jihadi Website Monitoring Group (JWMG), which summarizes and analyzes jihadist discourse on Web sites and forums, blogs and chat rooms.[1]
- A monthly database report summarizing and analyzing terrorism-related events worldwide.[2]

This and forthcoming cyber-desk newsletters will address two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse); and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack).

The following 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

We welcome brief articles from scholars and researchers engaged in the study of cyber-terrorism, cyber-crime, and electronic jihad. Interested researchers may submit articles for publication to ict@idc.ac.il. Articles will be peer reviewed. Those accepted for publication will be published under their author's name.

Sincerely,

Dr. Eitan Azani

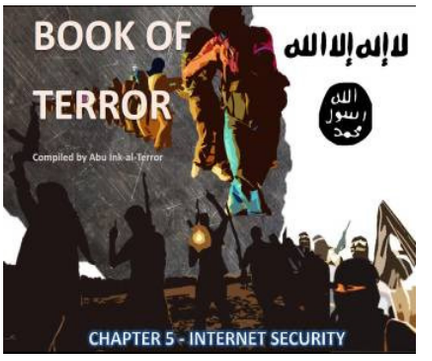
[1] www.ict.org.il/ResearchPublications/JihadiWebsitesMonitoring/JWMGPeriodicalReviews/tabid/344/Default.aspx.
[2] www.ict.org.il/ResearchPublications/DatabaseReports/tabid/380/Default.aspx.

**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.

*Defensive Tactics*

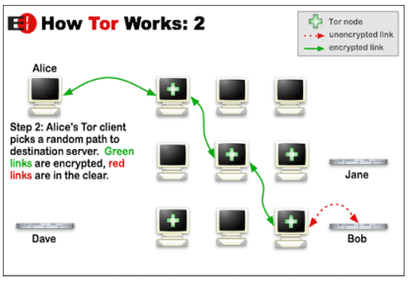
Encoding programs for organizations: A member of the jihadist Web forum Ansar Al-Mujahideen published a 172-page guide for English-speaking mujahideen on maintaining personal security when surfing the Internet. The guide included a detailed and illustrated explanation of how to use Asrar Al-Mujahideen, a message encoder, and other relevant programs. The person who posted the guide apologized to Arabic-speaking forum visitors that the guide was in English, and asked if anyone could translate it into Arabic and disseminate it more widely on the Internet.[3]




[3] http://www.as-ansar.com/vb/showthread.php?t=74657 (Arabic).

The administrator of the technical section of the jihadist Web forum Al-Minbar published a link to a video clip explaining how to use the Asrar Al-Mujahideen encoding program, which masks communication among mujahideen. In the past, Al-Qaeda in the Arabian Peninsula (AQAP) promoted the program as a means of communication among its members, as a vehicle for sharing "professional" information, and as a means of instructing Muslims everywhere, and especially in Europe, on perpetrating terrorist attacks against Western targets.[4]


Encoding programs for individuals: A member of the jihadist Web forum Ansar Al-Mujahideen provided a detailed explanation of how to use the TOR program to camouflage an IP address, so as to evade surveillance by espionage and regulatory agents.[5]




*Offensive Tactics*

Attacking Israeli Targets: A group of four hackers from Tunisia who call themselves "Fallaga Team" are apparently affiliated with global jihad. They maintain a Facebook page (http://www.facebook.com/FallaGa.tn) and a Web forum (http://forum.fallaga.com). During November 2012, Fallaga Team published the following:


- A video clip clarifying their choice of electronic jihad as the means of defending Muslims against various wrongs.[6]
- A video clip in support of the Palestinians, and decrying Israel's Operation Pillar of Defense against Hamas targets in the Gaza Strip. Fallaga Team promised to aid the Palestinians in the Gaza Strip by electronically attacking Israeli Web sites and Internet servers.[7]

[4] http://www.alplatformmedia.com/vb/showthread.php?t=15768 (Arabic).
[5] http://www.as-ansar.com/vb/showthread.php?t=75728 (Arabic).
[6] https://www.facebook.com/FallaGa.tn (Arabic).
[7] https://www.facebook.com/FallaGa.tn#!/photo.php?v=3950651127114&set=vb.397481643609586&type=2&theater.

- An announcement taking responsibility for hacking into multiple Israeli Web sites, including those of the Mossad, the Ministry of Foreign Affairs and the Kadima Party. Fallaga Team noted that anyone interested in hacking into Israeli Web sites should turn to the following Facebook page: https://www.facebook.com/events/124828247673713.[8]


- An announcement taking responsibility for hacking into the media Web site of the United Arab Emirates: https://more.etisalat.ae/index.html.[9]

A visitor to the jihadist Web forum Hanein reported that close to 100 Israeli Web sites had been sabotaged by a group of Moroccan hackers calling themselves Moroccan Agent Secret, as retaliation for Operation Pillar of Defense. Hanein's supervisor reported receiving information from Egyptian young people who were trying to paralyze the Web site of the Israel Police Force.[10]

Another visitor to the jihadist Web forum Hanein reported the sabotage of a Web site that markets military products – China Dacheng Body Armor – as revenge for China's massacre of its Uighur minority.[11]

*Key Topics of Jihadist Discourse, and Jihadist Propaganda, November 2012*[12]

Fighting Jihad: Al-Qaeda leader Ayman Al-Zawahiri called on Al-Qaeda's Al-Shabab Al-Mujahideen, the Somali people, and Muslims everywhere to wage jihad against the "Crusader campaign" of Kenyan Army and European Union forces against Somalia. Al-Zawahiri also published a statement of principle titled, "Aid to Islam". In

[8] http://hanein.info/vb/showthread.php?t=302152 (Arabic).
[9] https://www.facebook.com/FallaGa.tn#!/photo.php?fbid=509618879062528&set=a.397482876942796.98987.397481643609586&type=1&theater.
[10] http://hanein.info/vb/showthread.php?t=302153 (Arabic).
[11] http://hanein.info/vb/showthread.php?t=303287 (Arabic).
[12] 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.

it, he reminds all Muslims of their obligation to cleave to tawhid [monotheism], liberate occupied Muslim lands, and establish a caliphate

Abu Muhammad Al-Adnani, the official spokesperson for the Islamic State of Iraq, insisted that the latter was continuing jihad in Iraq, according to the plan outlined by its late founder, Abu Bakr Al-Baghdadi, with the aim of regaining control of the areas from which it had retreated. Al-Adnani boasted of that the plan was a success, and named several of the Islamic State of Iraq's gains against the Shiite government of Iraq. He promised that jihad would soon enter a new phase.

The Salafi-jihadist groups that have taken control of northern Mali are preparing to fight the international forces that are about to invade in an attempt to regain the region for the Malian government. Concurrently, Salafi-jihadists in Gao, northern Mali, announced that they had begun implementing Islamic law [shari'a] there.

Sheikh Abu Muhammad Al-Tahawi, a prominent Jordanian Salafi-jihadist, asked the Muslim nation to assist the Al-Nusra Front, an offshoot of Al-Qaeda in Syria, and hasten the fall of the Syrian regime.

Ahmad Ashush, a prominent Egyptian Salafi-jihadist, officially declared the establishment of the "Fighting Salafi Pioneers – Ansar Al-Sharia in Egypt".

Eulogizing Martyrs: In a video clip, Al-Qaeda leader Ayman Al-Zawahiri eulogized Abu Al-Walid Al-Maqdisi, a founder of the Palestinian Salafi-jihadist Shura Council of the Mujahideen in the Environs of Jerusalem, which is active in the Gaza Strip and the Sinai Peninsula.

Online Publications: The jihadist media outlet Fursan Al-Balagh published a new magazine titled, *Al-Balagh*.

**Cyber-Crime and Cyber-Terrorism, December 2012**

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")[13] Internet during December 2012. It is representative of online criminal activity during that period, and also sheds light on the behavior of terrorist organizations.

Credit Cards: An item that appeared on December 5, 2012 claims to have publicized the names and details on some 5,000 Israeli credit cards. Although all of the cards expired in March 2012, it should be noted that credit cards are usually renewed automatically.

An item was published by GrenXparta_Hacker, containing the full details of credit cards belonging to a resident of Belgium, and to two residents of Britain.

On December 21, 2012, Th3 M4RoC4in GhOsT published an item explaining a mechanism that automatically defiles valid credit card numbers.

An item was published by MagiCo Spam and DR Freedom containing detailed information about some 30 credit card holders, all of them from the US. The information appears to have been culled from multiple sources, and is not uniform. The data on the cardholders includes PayPal passwords, social security numbers, birth dates, names, full details of the credit cards (most of which are still valid), the cardholder's mother's maiden name, telephone numbers, email and street addresses, AOL account information, and bank account numbers.

An item was published containing the details of 19 credit cards and their owners, most of them from Britain and the US.

Data Leaks: On December 11, 2012, hackers from Saudi Arabia who have a Twitter account at @JM511 announced that they had sabotaged the servers of www.aurora-israel.co.il, a Spanish-language Web site about Israel and Judaism. The hackers stole the user names, email addresses, and passwords of both the site's administrators some 200 of its visitors.

[13] 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 Biddle, P., England, P., Peinado, M., and Willman, B. (no date), "The Darknet and the Future of Content Distribution", *Microsoft Corporation*, http://msl1.mit.edu/ESD10/docs/darknet5.pdf.

The www.yasam.co.il site was sabotaged by hackers, who exposed its database (including the structure and content of the nine tables comprising it). Data about at least eight clients and their credit cards were revealed. However, half of the credit card numbers were invalid (e.g., 541111111111111), and half of the cardholder's addresses (all of which were in Israel) were under the name "Yoni Rotenberg".

Online Attacks: On December 13, 2012, "the cyber warriors of Izz Al-Din Al-Qassam" took responsibility for an attack preventing decentralized services (DDoS) on the Web sites of several US banks and financial institutions. This attack had been preceded by an early warning posted by the group. The attack was apparently at least somewhat successful, as the sabotaged sites were reported to be suffering from slowed online and mobile phone activity, as problems of accessibility.

On December 21, 2012, "Anonymous" announced that Xc0unt3r, a member of the group of hackers known as Xl3gi0n, had hacked into the Web site http://btflive.net, which collects data on stock exchanges in the Middle East. According to Anonymous, the sabotage revealed details about the sites' administrators and hundreds their users around the Middle East. Previously, Xc0unt3r had hacked into the Web site www.unitycoalitionforisrael.org, leaking information on many hundreds of that site's members.

Spotlight on Trade in Counterfeit Medications: The Internet, primarily the "dark Web", is a lively market for the sale and purchase of medications – whether real or counterfeit. Consequently, it is vulnerable to the nefarious interventions of criminal organizations and, increasingly, terrorist organizations, which use counterfeit prescriptions, trade in prohibited medications, and even manufacture counterfeit medications.

During December 2012, it was reported that counterfeit medications from China were making it difficult to fight malaria in several African countries, primarily Tanzania and Uganda. Although no death toll was reported, it is believed that one-third of the anti-malaria medications being used in Africa are counterfeit or of inferior quality. It is thought that many of them originate in China.

**Case Study**

Each newsletter issued by the ICT's cyber-desk will discuss in greater detail a recent incident of cyber-attack. This issue highlights the nearly paralyzing attack of the "Shamoon" virus on the computers of two Middle Eastern oil and gas giants.

*A Cyber-Offensive against Saudi Arabia's ARAMCO, August 2012*

This past summer, several major Middle Eastern energy corporations were attacked by a deadly computer virus. Two of the chief victims of the virus, known as "Shamoon", were Saudi oil giant ARAMCO and Qatari RasGas.

Aramco, an oil and gas corporation owned by the Saudi Arabian government, was the first to be attacked, on August 15, 2012. Shamoon erased the content of more than 30,000 computers – more than 85% of Aramco's computers – causing serious harm. It took nearly two weeks to repair the damage. Fortunately, Shamoon attacked Aramco's administrative network, and not the network governing production or supply.[14] Abdallah Al-Sa'adan, Aramco's vice president for planning and the man responsible for investigating the attack together with the Saudi Ministry of the Interior, said that whoever had deployed Shamoon had meant to "stop the flow of oil and gas to local and international markets".[15] He called the virus an attack against the entire Kingdom of Saudi Arabia, and not only against Aramco.

Several weeks later, RasGas, which is located in Qatar, was attacked by the same virus. According to US Minister of Defense Leon Panetta, the attack was among the most destructive carried out in the private sector.[16] US sources further claimed that the attack had been perpetrated by Iran, as retaliation for the embargo on the export of Iranian oil.[17]

---

[14] http://english.alarabiya.net/articles/2012/12/09/254162.html.
[15] http://www.spacewar.com/reports/Saudis_and_allies_build_cyberwar_defenses_999.html .
[16] http://www.washingtonpost.com/world/national-security/cyberattack-on-mideast-energy-firms-was-biggest-yet-panetta-says/2012/10/11/fe41a114-13db-11e2-bf18-a8a596df4bee_story.html.
[17] http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html.

The Shamoon virus has three modules:[18] (1) Dropper, the main module, which contains the espionage files that infect computers; (2) Reporter, the module that controls, monitors, and reports the content of the infected computers; and (3) Wiper, the module that destroys the content of the infected computers.

Because Shamoon can proliferate, infecting multiple computers in the same network, it can also be characterized as a "worm". The Shamoon file contained a photograph of the burning of the American flag; this hints that its dissemination was politically motivated, most likely by a body that supports the Iranian government. Retroactive engineering analysis of Shamoon indicates that the programmers who designed the virus are good – but not excellent – and may even be amateurs. This is suggested by the large number of errors they made, some of which prevented Shamoon from working as planned.[19] Nevertheless, the deployment of Shamoon is an important test case, as it was not an act either of espionage or of crime. Rather, it was a cyber-offense: an attack meant to impede crucial computer-controlled processes, such as the worldwide supply of oil and gas.

[18] http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Sep2012.pdf.
[19] http://www.securelist.com/en/blog/208193834/Shamoon_The_Wiper_further_details_Part_II.