Capitol Hill Briefing

The Enemy Within: Where are the Islamist/Jihadist Websites Hosted and What Can Be Done About It?

July 19, 2007
Dear Friend of MEMRI,

Recent terror plots such as those against Fort Dix in New Jersey and against JFK International Airport, and the attempted car bombings in the United Kingdom, all have ties to Islamist websites that belong to Al-Qaeda as well as to other organizations.

You are invited to join us on Thursday July 19, 2007 from 9:30-10:30 a.m. in the Rayburn House Office Building Room 2200, for a presentation hosted by The Middle East Media Research Institute (MEMRI) on this issue.

The event has been organized in cooperation with Rep. Gary Ackerman (D-NY), chairman of the House of Representatives Foreign Affairs Subcommittee on the Middle East and South Asia and Rep. Mike Pence (R-IN), ranking member of the Subcommittee on the Middle East and South Asia.

In recent months, both Congressmen Ackerman and Pence have brought the issue of Islamist websites impacting the spread of terror around the world to the attention of their Congressional colleagues and the American public.

MEMRI President Yigal Carmon will speak about the issue of Islamist websites in the war on terror and the impact of the growing network of Islamist websites hosted in the U.S.

He will also discuss the overall importance of the Internet to extremist Islamists and how they make extensive use of this medium. Many of these Islamist websites are hosted in the U.S.

Exclusive video of Islamist websites will also be shown.

Sincerely,

MEMRI

About MEMRI’s Jihad & Terrorism Studies Project: Established in 2000, this project monitors groups that educate and preach jihad and martyrdom in mosques, schools, and in the media of the Middle East as well as in the West. As part of this project MEMRI has introduced the Islamist Website Monitor Initiative that monitors over 60 of most important terrorist websites, and directly serves as a vital research tool for the U.S. and its allies in the war on terror.
Congressman Mike Pence (R-IN)
Ranking member of the Subcommittee on the Middle East and South Asia

“Thank you Chairman Ackerman. I thank you for the opportunity to partner with you in this important public moment and I bring a special greetings to (MEMRI) President Yigal Carmon and the gathered guests today for the outstanding work of MEMRI and I hope today’s event sheds a light on the important work that you are doing. Since MEMRI was established in 1998 it has provided an invaluable window into an otherwise opaque situation to most Americans.

Even now the Middle Eastern and Islamic world is shrouded in mystery for too many. Since September 11 MEMRI has simply become indispensable. I think of MEMRI as an open source of intelligence for the public good. MEMRI relies on a dirty old trick, through expert translators and analysts, they quote various figures directly. Some of them howl in protest. The fact that MEMRI is controversial is partly proof of how effective an institution it is. Today MEMRI will demonstrate Jihadi websites widely available. We will see that sometimes they are hiding in plain site. MEMRI has done the hard work of locating and exposing them in their findings. Today will be troubling to millions of Americans. Today’s efforts are still another critical service for the public good. If MEMRI didn’t exist we would have to invent it. So I salute MEMRI and its President Yigal Carmon and hope they continue to shine the spotlight of truth on the Middle Eastern governments and media outlets in their own words. I will quote another great passage from Abraham Lincoln. He said, “Give the people the facts and the republic will be saved.” I suspect that much of the destiny of this republic is directly tied up in the American people and the people of the West knowing the heart and the intention of those that we face. MEMRI provides a critical window into that world and for that I am deeply grateful.”
I want to welcome everybody to this morning’s briefing which is being done by MEMRI, the Middle East Media Research Institute, in cooperation with the subcommittee on the Middle East and South Asia. My name is Gary Ackerman and I am the chairman of the subcommittee and I am joined by my good friend and colleague and ranking member of the subcommittee, Congressman Mike Pence from Indiana. It is a pleasure for both of us to work with MEMRI to make this briefing possible. I would like to say a few words of introduction then I will turn to Mr. Pence for any comments he would like to make and then introduce Mr. Yigal Carmon, MEMRI’s founder and president and he will conduct the briefing.

Terrorists come in a variety of flavors, all of them bitter and poisonous, but nevertheless there is a great range in their causes and motives. But they have in common a technique and a willingness to go beyond any law and decency or morality to achieve their ends. Not surprisingly, terrorists seek to use the laws and the rights that decent societies uphold as tools with which to conduct their various deeds. Freedom of speech, the foundation of democracy government, is thus converted by terrorists into a weapon with which they attack democracies. However, as President Lincoln reminded us, the constitution is not a suicide package and there is a considerable gap between political speech even offensive, hateful and disgusting speech, and the incitement to violence and conspiracy to commit acts of terror.

You will not find two stronger advocates of the first amendment than Mr. Pence and myself. He is a former broadcast journalist and I am a former newspaper publisher. We know what the first amendment means to our nation, to our people, and to our culture. America is not without free speech, but we also know terror when we see it and we know that the first job of a free government is to provide common defense. This task of reconciling national defense with free speech is not impossible. One has to delve into the details to be sure but there is more than enough legal space to distinguish between the argument and incitement between conspiracy theory and conspiracy fact.

Thanks to MEMRI, we can see what our enemies are saying, how they see the world, and how they see us. This open source of intelligence is invaluable. The challenge for us in government is to take this knowledge and to incorporate it into a broader strategic picture. The challenge before us is a serious one and to beat it we need to use all the tools we have. [With] public diplomacy and covert operations, international intelligence, and law enforcement cooperation, and sometimes with military force, we can prevail in this struggle, but only if our strategy is tuned correctly to the challenge and MEMRI has played a great part in helping us tune it more precisely.

Since 1998 Yigal Carmon has served as president of MEMRI, an institution that is a vital need in the security policy community here and throughout the world. Uniquely, MEMRI explores the Middle East and the media throughout the region. MEMRI bridges the language gap that exists between the West and the Middle East, providing timely translations of Arabic, Persian, and Turkish media as well as original analysis of political, ideological, intellectual, social, cultural, and religious trends of the Middle East. Never has this work been more timely or more important.
The Enemy Within: Where are the Islamist/Jihadist Websites Hosted, and What Can Be Done About It?
INTRODUCTION

Extremist Islam makes extensive use of the Internet, which serves it well due to its immense reach, impact, and capabilities. One can hardly imagine the immense growth of radical Islam and its jihadi organizations in recent years without the Internet. The threat posed by Islamist websites has recently been demonstrated by three cases: the case of the New Jersey group that planned a terrorist attack on Fort Dix; the planned terrorist attack on J.F.K., and the attempted car bombings in the UK. According to media reports, the terrorists in all three cases were inspired by jihadist websites. There were also two recent court cases in Britain and Switzerland in which terrorists were convicted of using Internet sites to promote terrorist activities.

The jihadist terrorist organizations utilize the Internet for two main purposes: for operational needs and for indoctrination and da’wa (propagation of Islam).

1. Operational Purposes

Islamist organizations use the Internet as a tool in the military training of jihad fighters by circulating military guidebooks on weaponry, battle tactics, explosives manufacture, and other topics. An example is Al-Qaeda’s online military magazine Mu’askar Al-Battar (The Al-Battar Training Camp), published by the Military Committee of the Mujahideen in the Arabian Peninsula.

Some websites also carry courses on manufacturing explosives and even guides for making homemade dirty bombs.

Another type of online operational activity is the use of hacking techniques to sabotage Internet sites – what the Islamists term “electronic jihad.” As part of this activity, Islamist hackers attack websites of those whom they consider their enemies with the aim of damaging morale, and attempt to hack into strategic economic and military networks with the aim of inflicting substantial damage on infrastructures in the West. Many Islamist websites and forums have special sections devoted to the topic of electronic jihad, such as the electronic jihad section in the Abu Al-Bukhari forum.

2. Indoctrination and Da’wa Needs

The main purpose for which the terrorist organizations use the Internet is for indoctrination and da’wa.
The organizations attach great significance to this Internet activity, as evident from the considerable efforts they invest in it. Al-Qaeda, for example, has an “information department” and a very active production company, Al-Sahab. Likewise, the Islamic State of Iraq (ISI) – which is an umbrella organization founded by Al-Qaeda, incorporating several terrorist groups in Iraq – has an “information ministry” and two media companies, Al-Furqan and Al-Fajr. In addition, there are independent media companies serving the Islamist organizations, such as the Global Islamic Media Front (GIMF), which denies having ties with Al-Qaeda but has posted Al-Qaeda statements taking responsibility for terrorist acts. The GIMF has also established the *Katibat Al-Jihad Al-I’lami* (Media Jihad Brigade).4

The online indoctrination and *da’wa* activities are regarded by the organizations as an integral part of jihad, and as another front of jihad in addition to its military, economic, and political fronts. In fact, they characterize online media or informational activity as a type of jihad that can be carried out by those who cannot participate in the fighting on the battlefield. They call this kind of jihad “the media jihad” (*al-jihad al-i’lami*) or “the *da’wa* jihad” (*al-jihad al-da’awi*).5

The following are some examples of websites that carry out indoctrination and *da’wa* activities by disseminating communiqués, religious tracts and videos that serve the terrorists’ purposes.

1. The Islamist forum called “World News Network,” which posts messages by numerous organizations. The following is a page from the website that includes messages by Al-Qaeda’s production company Al-Sahab, by the ISI media company Al-Furqan, and by the Iraqi terrorist organization Ansar Al-Sunna.

2. The Al-Saha forum, which posts videos produced by Al-Sahab and speeches by Al-Qaeda leaders, such as Al-Zawahiri.

3. Islamist websites sometimes have special sections devoted to messages by the jihadist media companies. For example, the Al-Nusra forum (which is affiliated with the Global Islamic Media Front – GIMF), has a special section devoted to GIMF messages.

In practice, the two types of online activity conducted by terrorist organizations – military activity and informational activity – are combined in that prominent terrorists play an active role in online media activities. For example, Fares Al-Zahrani, an Al-Qaeda leader who was arrested in August 2004 by the Saudi authorities, used to write on Islamist forums and on Abu Muhammad Al-Maqdisi’s website “Minbar Al-Tawhid Wal-Jihad” under the pseudonyms Abu Jandal Al-Azadi and Al-Athari.6 Another senior Al-Qaeda operative, Abd Al-Aziz Al-Anzi, who likewise participated in clashes with Saudi security forces, headed the Al-Qaeda Media Council, and was referred to as “the information minister of Al-Qaeda in the Arabian Peninsula,” was also very active online. He recruited Al-Qaeda supporters on Internet forums, and was a supervisor on the Al-Salafiyoon website (www.alsalafyoon.com), under the pseudonym Abd Al-Aziz Al-Bakri. He also wrote regularly for Al-Qaeda’s online magazine *Sawt Al-Jihad* (The Voice of Jihad), under various pseudonyms, among them Abdullah bin Nasser Al-Rashid, Abd Al-Aziz bin Musharraf Al-Bakri, Sheikh Nasser Al-Najdi, and Nasser Al-Din Al-Najdi.7
Some of the Arab countries in which Islamic extremists are most active employ highly restrictive supervision measures against individuals and groups involved in online terrorist activity. As a result, Islamist organizations and their supporters prefer to use Internet Service Providers (ISPs) in the West – and especially in the U.S., which is a key provider of Internet services – and thus exploit Western freedom of speech to spread their message.

In many cases, Western countries even host websites of organizations that have been officially designated by these very countries as illegal terrorist organizations. It must be stressed, though, that the ISPs themselves are frequently unaware of providing services to extremist elements.

The following are examples of jihadist websites hosted in the West (along with their URLs and the names of the ISPs that host them), in three main categories:

- Websites officially or unofficially associated with specific terrorist organizations
- Forums used by terrorist organizations
- Websites of sheikhs supporting terrorism

**Websites of Terrorist Organizations**

1. The website of the Iraqi organization Asaeb Al-Iraq, hosted in Texas.

   www.iraqiasaeb.org
   ISP: Layered Technologies, Inc., Texas
2. The website of the Jaysh Al-Mujahideen organization, hosted in Pennsylvania.

www.nasrunmiallah.net
ISP: Network Operations Center Inc., Pennsylvania, USA

3. The website of the Palestinian Islamic Jihad organization, hosted in Texas.

www.sarayaalquds.org
ISP: ThePlanet.com Internet Services, Inc., Texas, USA
4. A Pro-Hizbullah website, hosted in Texas.

5. A blog called “Supporters of Jihad in Iraq,” hosted in Washington state. The caption at the top of the page says “Kill the Americans everywhere.”
Islamist Forums

Currently, forums are the primary platform used by Islamist organizations to spread their messages. The importance that the organizations attach to these forums is evident in the fact that their official statements, such as communiqués or videos, are usually posted on their forums before being posted on their websites. For instance, Al-Qaeda, which has no official websites, uses Islamist forums to convey its messages.

The following are some examples of forums:

1. The highly popular Al-Hesbah forum, hosted in Texas.

![Al-Hesbah Forum](image)

www.alhesbah.org
ISP: RealWebHost, Texas, USA

2. The Al-Tajdid forum, hosted in Germany.

![Al-Tajdid Forum](image)

www.tajdeed.org.uk
ISP: FASTHOSTS-UK-NETWORK, United Kingdom
3. The Al-Saha forum, hosted in Germany.

http://alsaha2.fares.net
ISP: Liquid Web, Inc., Michigan, USA
Websites of Sheikhs Who Support Terrorism

Known Islamist sheikhs play a pivotal role in setting up the organizations’ ideological infrastructure, and in granting religious-legal legitimacy to their activities. Many of these religious scholars are currently serving prison sentences for incitement to terrorism or even for active involvement in terrorism. However, this does not prevent them from spreading incitement and supporting terrorism via their websites, which remain active, and are often hosted in the very same counties that convicted and imprisoned them. For example:

1. The website of Abu Qatada Al-Falastini (a.k.a. Omar Mahmoud Abu Omar), a Jordanian of Palestinian origin, who has been detained in Britain since 2005 on suspicion of having ties with Al-Qaeda. His site is hosted in Britain.

   www.almedad.com/tae
   ISP: BT-Wholesale, U.K.

2. The website of Sheikh Abu Muhammad Al-Maqdisi, who was the spiritual mentor of the late commander of Al-Qaeda in Iraq, Abu Mus’ab Al-Zarqawi. Al-Maqdisi’s website includes numerous documents that provide ideological and religious-legal legitimacy for many Islamist terrorist organizations.10

   www.tawhed.ws / www.alsunnah.info;
   ISP: Interserver, Inc., New Jersey, USA
3. The website of extremist Islamist Sheikh Hamed Al-Ali, known for his support for jihad fighters.

www.h-alali.net;
ISP: FortressITX, New Jersey, USA
Sites Using Services Provided by the Largest Internet Companies Google, Yahoo! and MSN

Terrorist organizations and their supporters also use services offered by the large Internet companies Google, Yahoo! and MSN. The following are examples of blogs hosted by these companies that disseminate terrorist messages:

First, two blogs hosted by Google:

1. The unofficial blog of “Al-Furqan Media,” the production company of the Islamic State of Iraq (ISI), which was founded by Al-Qaeda.

   www.gldag.blogspot.com;
   ISP: Google Inc., California, USA

2. A blog dedicated to the legacy of the former leader of Al-Qaeda in Iraq, Abu Mus’ab Al-Zarqawi, which includes Al-Zarqawi messages and videos.

   www.kjawd.blogspot.com;
   ISP: Google Inc., California, USA
3. A Yahoo! group called Supporters of Jihad in Iraq.

http://groups.yahoo.com/group/ansaraljehad;
ISP: Yahoo! California, USA

4. A pro-Hizbullah group on Microsoft’s portal MSN which posts speeches by Nasrallah, information on Hizbullah operations and links to other Hizbullah sites.

http://groups.msn.com/Hizbullahh/page16.msnw;
ISP: Microsoft Corp., Washington, USA
Websites in European Languages:

The jihadist websites hosted in the West are not always in Arabic. Some are in European languages such as English, French and German.

Examples:

1. An English section on the forum called “World News Network.”

![World News Network](image1)

www.w-n-n.net;
ISP: SiteGenie, LLC, Minnesota, USA.

2. GIMF’s German website, hosted in Britain:

![GIMF's German website](image2)

http://gimf1.wordpress.com;
3. A Website in French called La Voix des Opprimés (The Voice of the Oppressed), hosted in the U.S.

http://news.stcom.net;
ISP: DNS Services, Florida, USA.
WHAT CAN BE DONE?

The prevalent view in the West, even among officials in charge of counterterrorism, is that the primary way to fight the jihadist websites is to spread an alternative message, or a “counter-narrative,” which is opposed to that of the Islamists. Indeed, Islamist ideology should and can be countered by alternative messages. However, such an ideological campaign is, by its very nature, a long-term effort with no immediate results.

More effective and immediate ways to fight the phenomenon are, firstly, to expose the extremist sites via the media, and thus to inform ISPs and the public at large of their content. Secondly, to bring legal measures against ISPs that continue to host extremist websites and forums.

Exposure

Experience teaches that exposure is, in itself an effective measure against extremist sites. In 2004, MEMRI published a comprehensive two-part review of Islamist websites and their hosts. Within a week of the publication of this review, most of the sites exposed in it were closed down by the ISPs that hosted them.

This suggests that an effective measure against the extremists’ online activities would be to establish a database – governmental or non-governmental – which would routinely publish information about extremist sites, and/or provide it to ISPs upon request. This database would be similar to government bodies that inform the public on various issues vital to its safety – such as bodies that issue weather alerts and travel advisories; the Better Business Bureau, which provides businessmen with information about individuals and companies convicted of fraud; or the US Treasury’s Office of Foreign Assets Control that provides information to banks, which are bound by the regulation of “know your customer.”

It should be stressed that the ISPs have a legal authority to remove sites that violate the law (e.g. the copyright laws) or sites that abuse the ISPs own regulations. Thus, with information on extremist sites at their disposal, the ISPs should have both the ability and the obligation to remove such sites from their servers.

Legal Countermeasures

As for legal countermeasures, the prevailing opinion among the American public – and even among government officials, including those in charge of counterterrorism – is that the First Amendment severely limits the scope of legal measures that can be brought against terrorist websites. But the fact is that the American legal code contains clear and effective provisions against terrorist organizations and their online activities, including the following:

Designated Foreign Terrorist Organizations

The U.S. officially designates certain organizations as “Foreign Terrorist Organizations” (FTO) and certain individuals as “Specially Designated Terrorists” (SDT) or “Specially Designated Global Terrorists” (SDGT). The list of designated organizations and individuals is updated regularly and made available to the public.

These designations have legal consequences. For example, section 219 of the Immigration and Nationality Act states that it is unlawful to provide a designated FTO with “material support or resources,” including “any property, tangible or intangible, or services,” including “communication equipment and facilities.”

Some of the organizations and individuals listed in this document – such as the Islamic Jihad organization, for example – are designated FTO and SDGT, which means that the ISPs hosting their sites are clearly violating U.S. law.

18 U.S.C. Section 842

Another pertinent law is Title 18, Section 842, of the U.S. Code, which states: “It shall be unlawful for any person to teach or demonstrate the making or use of an explosive, a destructive device, or a weapon of mass destruction, or to distribute by any means information pertaining to ... the manufacture or use [thereof] with the intent that the teaching, demonstration, or information be used for, or in furtherance of, an activity that constitutes a Federal crime of violence.”
Websites and forums that disseminate operational military information to terrorists, such as many of the sites and forums presented here, are illegal under this law, even if they are not formally associated with a designated FTO.

A motion claiming this law to be incompatible with the First Amendment was denied by an American court in the case of Rodney Adam Coronado, a radical animal-rights and environmental activist. Coronado was convicted of violating Title 18, Section 842 after giving a lecture in California in which he showed how to build an incendiary bomb. After being charged, Coronado filed a motion to dismiss the case against him on grounds that the law had violated his First Amendment rights. The motion, however, was denied by the District Court of San Diego. In explaining its ruling, the court stated that “the First Amendment does not provide a defense to a criminal charge simply because the actor uses words [rather than actions] to carry out his illegal purpose...”

*Y. Carmon is the President of MEMRI, Y. Yehoshua is Director of Research at MEMRI, E. Alshech is Director of the Jihad and Terrorism Studies Project at MEMRI, D. Hazan is Director of the Islamist-Jihadi Website Initiative at MEMRI, and R. Carmon is a Research Assistant at MEMRI.

Notes


5See article by Nur Al-Din Al-Kurdi in the third issue of the magazine *Dhurwat Sanam Al-Islam* (referring to jihad), issued by the Information Division of Al-Qaeda in Iraq.


8Saudi Arabia, for example, passed a bill in March 2007 that stipulates imprisonment of up to 10 years and/or a fine of up to 5 million riyals for anyone setting up a website for a terror organization or a site promoting terrorist goals.

There have also been arrests. On June 5, 2007, the Saudi Security services detained three Al-Qaeda members for using the Internet to spread extremist ideology and recruit young people to jihad. One of the detainees was Abu Asid Al-Faluji, who attempted to recruit youths for terrorist operations and disseminated via the Internet speeches by bin Laden and Abu Mus’ab Al-Zarqawi; another was Abu Adullah Al-Najdi, who was involved in terrorist operations against Saudi Arabia and attempted to publish a new edition of the e-journal of Al-Qaeda in Saudi Arabia, Sawt Al-Jihad, which was closed down two years ago. (*Al-Watan*, Saudi Arabia, June 6, 2007; *Al-Riyadh*, Saudi Arabia, June 7, 2007).

9All data concerning the websites was verified June 1, 2007.


11Measures of this sort were the focus at a May 3, 2007 hearing of the Homeland Security and Governmental Affairs Committee, chaired by Senator Joseph Lieberman, which dealt with “The Internet as a Portal for Islamist Extremists.” The speakers at this hearing – Lieutenant Colonel Joseph Felter from the United States Army; Deputy Assistant Secretary of Defense Michael Doran; and Frank J. Cilluffo, Director of the Homeland Security Institute at George Washington University – emphasized that, in order to counter the Islamist threat, the West must “win the battle for hearts and minds and offer hope... to those who might otherwise be seduced by the jihadi ideology,” to quote Frank Cilluffo. As examples of activities that achieve this aim, Cilluffo mentioned, among other things, the Indonesian pop-star Ahmad Dhani who “uses his music to counter calls to violence with a message of peace and tolerance,” and an anti-terrorism fatwa issued in 2005 by the Figh Council of North America – a pro-Islamist body.


14For an updated list of Specially Designated Nationals, see: http://www.treas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf.

If you want to know the content of an Arabic-language website hosted by your company, please fill out the following form.

MEMRI's language experts will contact you in about a week with information about the site.

*Denotes required field

Please do NOT contact MEMRI after submitting a site for review. MEMRI will contact you approximately one week after receiving your information.

Thank you.