U.S. STRATEGY FOR COUNTERING JIHADIST WEB SITES

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, NONPROLIFERATION AND TRADE

OF THE

COMMITTEE ON FOREIGN AFFAIRS HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

SEPTEMBER 29, 2010

Serial No. 111–130

Printed for the use of the Committee on Foreign Affairs

Available via the World Wide Web: http://www.foreignaffairs.house.gov/

U.S. GOVERNMENT PRINTING OFFICE
61–516PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON FOREIGN AFFAIRS

HOWARD L. BERMAN, California, *Chairman*

GARY L. ACKERMAN, New York
ENI F.H. FALEOMAVAEGA, American Samoa
DONALD M. PAYNE, New Jersey
BRAD SHERMAN, California
ELIOT L. ENGEL, New York
BILL DELAHUNT, Massachusetts
GREGORY W. MEEKS, New York
DIANE E. WATSON, California
RUSS CARNAHAN, Missouri
ALBIO SIRES, New Jersey
GERALD E. CONNOLLY, Virginia
MICHAEL E. McMAHON, New York
THEODORE E. DEUTCH, Florida
JOHN S. TANNER, Tennessee
GENE GREEN, Texas
LYNN WOOLSEY, California
SHEILA JACKSON LEE, Texas
BARBARA LEE, California
SHELLEY BERKLEY, Nevada
JOSEPH CROWLEY, New York
MIKE ROSS, Arkansas
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia
JIM COSTA, California
KEITH ELLISON, Minnesota
GABRIELLE GIFFORDS, Arizona
RON KLEIN, Florida

ILEANA ROS-LEHTINEN, Florida
CHRISTOPHER H. SMITH, New Jersey
DAN BURTON, Indiana
ELTON GALLEGLY, California
DANA ROHRABACHER, California
DONALD A. MANZULLO, Illinois
EDWARD R. ROYCE, California
RON PAUL, Texas
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
JOE WILSON, South Carolina
JOHN BOOZMAN, Arkansas
J. GRESHAM BARRETT, South Carolina
CONNIE MACK, Florida
JEFF FORTENBERRY, Nebraska
MICHAEL T. McCAUL, Texas
TED POE, Texas
BOB INGLIS, South Carolina
GUS BILIRAKIS, Florida

Richard J. Kessler, *Staff Director*
Yleem Poblete, *Republican Staff Director*

Subcommittee on Terrorism, Nonproliferation and Trade

BRAD SHERMAN, California, *Chairman*

GERALD E. CONNOLLY, Virginia
DAVID SCOTT, Georgia
DIANE E. WATSON, California
MICHAEL E. McMAHON, New York
SHEILA JACKSON LEE, Texas
RON KLEIN, Florida

EDWARD R. ROYCE, California
TED POE, Texas
DONALD A. MANZULLO, Illinois
JOHN BOOZMAN, Arkansas
J. GRESHAM BARRETT, South Carolina

CONTENTS

Page

WITNESSES

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

APPENDIX

U.S. STRATEGY FOR COUNTERING JIHADIST WEB SITES

WEDNESDAY, SEPTEMBER 29, 2010

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TERRORISM,
NONPROLIFERATION AND TRADE,
COMMITTEE ON FOREIGN AFFAIRS,
Washington, DC.

The subcommittee met, pursuant to notice, at 1:30 p.m., in room 2175, Rayburn House Office Building, Hon. Brad Sherman (chairman of the subcommittee) presiding.

Mr. SHERMAN. I want to thank our witnesses for being here.

I know that the title of this hearing uses the term "jihadist," which is widely used in the intelligence and antiterrorism community. I realize that the term "jihad" is sometimes used in Islam to describe a personal struggle; and, accordingly, I will use the word "terrorist" or "extremist," not that the term "jihadist" does not also carry with it the meaning, but it has secondary and tertiary meanings as well, and obviously those engaged in a personal reflection and struggles to improve themselves are not the focus of these hearings.

We have seen extremists use the Internet for a growing number of activities, including recruitment, propaganda, psychological warfare, and soliciting financial support. Today's hearing is to focus on how to best counter those activities and basically to ask the question: Why aren't we doing so?

The growing number of instances in which the Internet is used for extremist activity is quite long. For example, in March, the Washington Post reported that extremists used the Internet to pass along U.S. operational information to insurgents in Iraq. Perhaps the best-known example is Major Hasan, the Fort Hood shooter who was influenced by extremist propaganda on the Internet. The five men in Northern Virginia who traveled via Pakistan to attack U.S. troops in Afghanistan made contact with the extremist organization over the Web as well.

We see groups like Fajr, which not only maintain their own Web site but have a dedicated nexus to communicate with other extremist groups. One can find the many books and essays pushing the extremist position on the line, and you can find instructions on how to download extremist content onto your cell phone.

The question is, what is our response? The politically correct response is for us to monitor what is going on and maybe detect who is visiting these sites. We did a great job of determining which sites Major Hasan visited after the terrorist incident. Keep in mind that our enemies have decided that, even though we have the capacity to monitor, the Internet serves their purpose. So those that argue that our ability to monitor means that extremist Web sites are helping us more than they are helping our enemies have got to reflect on the fact that our enemies have analyzed this and come to the exact opposite conclusion. The other approach, also politically correct, is to reply, read everything on the Internet, and write an essay as to why the extremists are wrong and we are right.

Both of these responses to terrorists' use of the Internet have a number of advantages. They are polite, they are politically correct, and they involve hiring many people with master's degrees in foreign affairs. Being polite and hiring lots of people with master's degrees in foreign affairs may be the chief mission of our State Department and other national security bureaucracies.

I would prefer to see us shut down these sites. Now, you can argue the First Amendment, but the fact is that while you cannot scream fire in a crowded theater, you also cannot legally try to raise money for terrorists or provide an article how to "Make a bomb in the kitchen of your mom" or advocate that people do so. What we are talking about here are sites that are not protected by the U.S. First Amendment.

The advocacy of taking violent action against Americans certainly poses just as great a danger as yelling "fire" in a crowded theater. We are going to be told that there are lots and lots of Web sites, that is true, but they tend to get their content from 5 or 10 or 15 providers. So if we should down every Web site that provides original content, we will have shut down the propaganda machine, the finance machine, the recruitment machine that the terrorists are deploying on the Internet.

Now, private citizens have been working to shut down extremist Web sites by contacting companies who host these Web sites and urging them to take them down. In addition, the U.S. military, in at least one publicly reported case, decided to shut down a Web site.

I am going to try to save some of your time by skipping some of my prepared remarks here.

Yet we still have not only the many examples I mentioned before, but also Colleen LaRose, commonly called Jihad Jane, who was arrested in Philadelphia after months of trying to recruit jihadist extremists in the United States. The Los Angeles Times reports that this individual was just one of a dozen domestic terrorist cases that the FBI disclosed in 2009, all of which used the Internet as a tool.

Anwar al-Awlaki, an extremist leader with ties to al-Qaeda, is now being credited as being the brains behind online recruitment, particularly in a magazine written in English. I mentioned his most famous article regarding making a bomb in a kitchen.

The terrorists very much want to recruit operatives that are legally entitled to be in the United States and culturally familiar with the United States so that they can act without creating suspicion. The best and easiest way for them to reach out to American citizens, legal residents, and those familiar with our culture is through the Internet.

During the Bush administration, the military began formulating plans for a cyberattack to shut down a Saudi Web site, which they reportedly did. Interestingly, the Web site, according to the Washington Post, was being operated by a joint Saudi-CIA operation in order to collect intelligence on the extremists and possible Saudi insurgents. A better degree of coordination might be called for in our efforts.

There is, of course, the naming and shaming, trying to get Web site providers to take down certain Web sites. This is not always successful. We have people here with technical expertise who can perhaps advise us on whether the United States can do what we are told high school students are able to do, and that is to take down a Web site. And as I pointed out, we could take, remove the content from hundreds of Web sites if we were able to take down 5 or 10 other sites that are providing the content.

Now, it is attractive to say, well, we should just read what the jihadists put up or what the extremists and terrorists put up and then respond. Because a lot of us grew up in politics, and when you have a good argument, you prevail. I have never had an argument good enough to get 99 percent of the people in my district to agree with me and only 1 percent to agree with my opponent.

But if I ever did come up with such a good argument, that would be fine for my electoral purposes, but it wouldn't be successful here. Because if 1 percent of those visiting these Web sites do what the Web site authors want them to do, which is to become terrorists, then the fact that 99 percent are convinced to do otherwise hardly provides us with much solace.

The only way to be 100 percent convinced or 100 percent sure that 100 percent of the people who are visiting a Web site are not persuaded by it is to make sure that nobody is visiting the Web site. Anything else leaves you struggling to get 50, 60, 70 percent of the people who are visiting that Web site to not be convinced by it. So I look forward to using these hearings to see whether we are going to be a polite country or a safe country.

With that, I yield to the distinguished ranking member from Orange County, California, Mr. Royce.

Mr. ROYCE. Thank you, Mr. Chairman.

I followed your argument there on the percentages, but I thought it was interesting because I saw a story the other day out of Pakistan that indicated that only 2 percent of people in Pakistan believe that al-Qaeda was responsible for 9/11. So perhaps the environment is even less conducive in terms of trying to make a case when you are dealing with people that have so much disinformation.

One of the questions all of us have is how is it possible that this very dangerous jihadist ideology is spreading. The argument that the heart of this is really being spread through the Internet is an interesting one. I know personally from conversations that I have had with a number of people who have been radicalized that that played a key role, that that was at the heart of how they came to these conclusions.

I think it is following the way in which this is being used not only as a tool to recruit and indoctrinate but the way that, beyond that, it is becoming sort of a virtual radical Madrassa, these Deobandi schools that we see in Pakistan. Now we have these on the Internet. They are walking people through this logic or this argument, and they are being used to fund-raise, they are being used to train, they are being used to plot attacks. And if we think about 9/11, you know, al-Qaeda used an extremist Web site to help plot that 9/11 attack.

Today Hezbollah is particularly adept. Following up on that competing terrorist organization, they have become adept at doing this; and, obviously, it is done pretty cheaply. So you have got really a virtual caliphate, as somebody once mentioned here. Obviously, many are using these Web sites to target Americans with apparent success.

We had the 9–11 Commission report recently by Tom Kean and Lee Hamilton. From time to time, they make pronouncements on, you know, the current state of play and the war on terror and they have warned about complacency about home-grown terrorism and they said we have been—their words—"stumbling blindly" trying to combat it.

We see the ever steady pace at which this recruiting and these attacks are increasing. The report that was filed by the members of the commission said they found it—again, their words—"fundamentally troubling" that there is no Federal Government agency or department specifically charged with identifying the radicalization and recruitment of Americans into this process of being radicalized and then becoming terrorists. And, of course, it is the Internet that is central to that radicalization and recruitment.

So what to do about these Web sites? There is a debate about whether they should be taken down or whether they should be monitored, as the chairman referenced.

Intelligence can be gained on occasion, but we need the tools and focus to aggressively attack these sites. At the end of the day, we are at war. It is a declared war on the other side. They have declared war on the U.S., and we should act like we understand that. We should respond to that. One witness offers legislative suggestions that I look forward to hearing.

I commend Mr. Poe, my colleague, who is not with us yet for this hearing. He contacted YouTube, and he expressed his concern over the rise of terrorist groups posting on it after he witnessed some of these videos.

Some argue that we should be actively monitoring to counter radical Internet messages, debating some of these finer points over the justification of terrorist acts, for example. I understand the concept, but I don't know if our Government has the ability to effectively execute such a policy which requires a set of specialized and uncommon skills and very deep understanding, if you are thinking about somebody sitting there engaged in this kind of a debate. We should know also, I think, that a bad effort at this would do us harm. If we tried to do this and do it badly, we would be in more trouble.

One academic calls radical Islam on the Internet "a virtual community of hatred." How you embark on this is a very difficult question and they are very tough waters for a bureaucracy to dive into.

Given that they have declared war on us on the Internet, the answer is to take them down. The answer is the obvious answer, don't give them the ability to continue to recruit and to plan. I would have a bit more confidence if the administration better understood the totalitarian ideology that we are facing.

Six years ago, the 9–11 Commission found that “we are not threatened by ‘terrorism,’ some ‘generic evil’ but specifically by ‘Islamist terrorism.’ ”

This remains the threat today, but the commission’s straight talk is shunned by this administration which prefers to speak of “violent extremism.” That’s the very generic threat that the commission rejected. They wanted to name this threat for what it was. This blindness is one reason, perhaps, that we are “stumbling blindly,” as Kean and Hamilton regrettably concluded.

Mr. Chairman, I yield back.

Mr. SHERMAN. I wonder if we have an opening statement from the vice chairman of the committee.

Mr. SCOTT. Well, I will be very brief, but I would like to make a couple of statements about this very timely and important issue.

I think if there ever was an example of our becoming servants of the machines that were created to serve us, this is clearly an example of it.

The Internet sort of reminds me of the rope that is thrown down to a man fallen from a cliff. He can either use that rope to pull himself up or use that rope to hang himself.

The Internet and the use of it by terrorists and criminal activity is just mushrooming, and we have got to have the ability to be able to adapt our capability of thwarting the terrorists’ use of it as quickly as we can.

The topic of today’s hearing is one of increasing importance as we move through the 21st century and as we continue our offensive against terrorist groups, be they foreign or jihadist, including al-Qaeda, or domestic, as more and more are rapidly becoming.

The rise of social network and communications platforms like Facebook, Twitter, all allow for great, creative, and political and economic promise for all of us. It could be a rope to pull ourselves up.

But as we have seen all over the world, political movements and demonstrations have been organized through such Internet portals from the streets of Tehran to right here in Main Street, U.S.A. Spreading messages to the masses has become far easier in our interconnected world, and we have got to make sure that the United States, our country, remains at the forefront of the developing cyberworld in order to advance our Nation’s interests and to promote freedom and democracy abroad.

Likewise, this case of communications allows for enemies of our basic freedoms, enemies of democracy, to recruit for their destructive causes. While pursuing our strategic communications, encountering the recruitment attempts of terrorist groups, we also must make sure that we don’t use this to hang ourselves, that our vigilance is tempered by our respects to those rights that are endowed by our Creator, that we cherish and that are enumerated within our Constitution, the values that we represent.

And this is what I believe should be our primary focus in this hearing today. It is a delicate balance I think that we walk.

We have got to be able to intercept and unscramble encrypted messages. But we have got to balance it. We have got to balance our security needs with protecting the privacy, with protecting the democracy, protecting the freedoms.

Inherent in that freedom is our individual citizen's right to privacy. So we have got a challenge here and let us hope that at the end of the day that we use this rope we have to indeed pull ourselves up to a better country, a better world, and not allow it to hang us.

With that, Mr. Chairman, I yield back.

Mr. SHERMAN. Mr. Manzullo, do you have an opening statement?

Mr. MANZULLO. No.

Mr. SHERMAN. I should note that both witnesses and members will have 5 business days or longer, if they ask me for it later, to put their full statements in the record.

I should also say—just to clarify things—I think we are all talking about the same enemy, that is to say, those who believe in the use of terrorism or other violent means and are inspired by a corrupted interpretation of Islam and a corrupted interpretation of the concept of Islamic jihad.

First, I would like to introduce our first witness, Mansour Al-Hadj. He is the director of the Reform in the Arab and Muslim World Project for the Middle East Media Research Institute, MEMRI. Please proceed.

STATEMENT OF MR. MANSOUR AL-HADJ, DIRECTOR, REFORM IN THE ARAB AND MUSLIM WORLD PROJECT, THE MIDDLE EAST MEDIA RESEARCH INSTITUTE

Mr. AL-HADJ. Mr. Chairman, Ranking Member Royce, and distinguished members of the subcommittee, thank you for allowing me to serve as a panelist on this important topic.

My name is Mansour Al-Hadj. I was born and raised a devout Muslim in Saudi Arabia. I earned my degree in Sharia and Islamic Studies at the International University of Africa in Sudan.

I am the director of MEMRI's Reform in the Arab and Muslim World Project. My work involves focusing on liberal voices and advocates of reform in the Arab and Muslim world, including those who speak out against online jihad.

As a youth, I was taught to hate America, the West, Jews and Christians. I was taught to love jihad and those who wage it. Religious settlements and Islamist pamphlets turned me into an extremist by teaching me that Muslims are backward because we don't implement Sharia.

My transformation away from extremism came after reading the writing of a peace activist who denounced violence and supports the use of nonviolent means of social change. Today, I see many Muslims stuck in the same conflict I was. The difference is that today Muslims have much more access to the source of extremist ideas online through jihadist forums and Web sites.

Jihadist forums on Web sites have played a role in several recent terror acts in the United States such as the Fort Hood shooting and the failed Times Square bombing. I personally witnessed the powerful effect a propaganda campaign can have on a young mind. As a student in Sudan, one government recruitment effort during the civil war was a jihadist TV series. This show documented jihadi fighters imparting their love for jihad. I still remember how fascinated I was by their stories and how I longed to become one of them.

Just as the Sudanese Government managed to market the war to recruit thousands to join their jihad, terror organizations such as al-Qaeda are actively recruiting thousands through the Internet. Islamist organizations primarily use the Internet for spreading their message and propaganda. It is considered to be an integral part of their jihad, and they invest tremendous resource in it.

It is impossible to imagine the development of global jihad movement without the Internet. Through MEMRI's research of jihadi Web sites, it has discovered that many of them are hosted by Internet service providers in the U.S. that are unaware of the content due to the language barrier.

MEMRI addressed Congress on this issue in July, 2007. We suggested dealing with the problem by notifying ISPs in the United States about what they host in the hope that they would voluntarily remove the sites. In the week that followed, 32 out of 50 ISPs questioned removed the jihadi sites.

Opposition to closing these sites came in several varieties. First Amendment rights, the Web sites are a source of valuable intelligence, and the difficulty in dealing with a large number of Web sites were all given as a reason to keep the sites active.

However, we at MEMRI believe that if the key jihadi Web sites are shut down, the rest of them will dry up. Most importantly, the number of jihadist Web sites has decreased in recent years. Currently, the number of highly dangerous sites is less than 10.

It is important to mention that terrorist organizations are always on the lookout for other channels to propagate their ideology. As jihadists encounter increasing difficulty with their Web sites, they discovered Western social media outlets such as YouTube, Facebook, and Twitter.

In fact, YouTube is a primary clearinghouse for one of America's most wanted terrorists, Anwar al-Awlaki, who provided spiritual guidance and inspiration for several recent successful and failed terror attacks in the U.S. al-Awlaki's's presence in YouTube is the result of the shutting down of his Web site shortly after the Fort Hood shooting.

At that time, MEMRI reported that al-Awlaki's Web site was hosted by an ISP in California. Within 2 hours of the report's publication, the ISP removed al-Awlaki's Web site.

In conclusion, online jihad is a dangerous foe. The U.S. must confront it exactly as it confronts other forms of extremism on other fronts around the world, both within and beyond its border. As with its military ventures, the U.S. must initiate cooperation with its allies, international organizations, and the business community. Experience shows that this can indeed be done.

Mr. Chairman, this concludes my opening remarks. Thank you again for inviting me today. I welcome any questions that you or the members may have.

[The prepared statement of Mr. Al-Hadj follows:]

United States House of Representatives
Committee on Foreign Affairs, Subcommittee on Terrorism,
Nonproliferation and Trade

"U.S. Strategy for Countering Jihadist Websites"

September 29, 2010

THE MIDDLE EAST MEDIA RESEARCH INSTITUTE •
MEMRI
ميمري

Mansour Al-Hadj
Director of Democratization in Arab & Muslim World Project
The Middle East Media Research Institute (MEMRI)

www.memri.org

> "The average Muslim does not need to go to Afghanistan or Pakistan in order to attend training camps and learn how to fight the American enemy. Likewise, he does not need to be an expert or professional in making bombs and explosives to attack the U.S., as a bomb can easily be made using readily available materials such as nitrate, fertilizers that are sold in stores, agricultural materials, and a few canisters of gas and benzene.
>
> "Anyone can obtain these materials and make a bomb. Anyone can learn how to do it by searching the Internet and watching videos that explain how to make bombs from readily available materials – and then plant it in a pre-planned location, and detonate it with a remote device or a cellular phone, without leaving any traces behind him.
>
> "Anyone can obtain a firearm and open fire on a military base or an FBI or police headquarters, or on [the Capitol building], the Pentagon, the White House, or any other place. This can be done by a man, woman, child, student, teacher, university professor, doctor, lawyer, or anyone [else]."
>
> *- A post on the jihadist website Al-Shumukh by "Shamikh Muharrid," from a document titled "Woe to America: New Jihad Fighters That Intelligence Apparatus Cannot Trace." May 13, 2010*

******

Chairman Sherman, Ranking Member Royce, and distinguished Members of the Subcommittee, thank you for allowing me to serve as a panelist on this important topic.

A Journey from Extremism to Liberalism

My name is Mansour Al-Hadj. My parents are Muslims from Chad, but I was born in Mecca, Saudi Arabia, less than a mile from the Grand Mosque. I grew up in Jeddah and went to elementary school and middle school there. I spent my high school years in Chad. The following year I traveled to Sudan, where I got a degree in Sharia and Islamic Studies at the International University of Africa.

I came to the United States five years ago, after winning what was essentially a Green Card lottery. About two years ago, I started working for MEMRI, and today I am director of its Reform in the Arab and Muslim World project. My work involves focusing on liberal voices and advocates of reform in the Arab and Muslim world, including those speaking out against online jihad. One notable example includes Al-Arabiya TV director-general Abdul Rahman Al-Rashed, one of the most esteemed voices in the Arab media, who stated that there is a need "to wage war against extremist websites in general, which have become larger camps than the first camp that gave its name to the 'Al Qaeda' organization."

I was raised an observant Muslim. In school I was taught to hate America, the West, Jews, and Christians. In Koran school I was taught to love jihad and those who wage jihad for the sake of Allah. What really turned me into an extremist were the tapes of religious sermons that I would listen to – distributed at no charge by the Koran school – and the Islamic pamphlets that I would read. Most of them extolled the courage of the Arab and Afghan *mujahideen* who had fought the Soviets in Afghanistan, and described the miracles they had witnessed on the battlefield. I also would listen to Islamic songs ("Anasheed Islamiyah") bemoaning the sorry state of the Muslims worldwide, extolling the virtues of jihad and martyrdom, and depicting the West as the cause of every problem and catastrophe in the Muslim world.

During this period of my youth, I longed to discover the true Islam, and I was troubled by an apparent paradox: If we Muslims have the Koran, which guides us in the path of truth and righteousness, how is it that we are so backward? The songs and books gave me an answer: they taught me that we Muslims are backward because we do not follow the directives of Islam and the Sunna – the Prophet Muhammad's sayings and customs – and do not implement the Sharia - Islam's sacred law – as the Prophet Muhammad did.

After graduating from university in Sudan, I returned to Saudi Arabia. I was confused and had many questions about Islam and its role in my life. But I was afraid to ask because I was taught that a true believer never questions Allah.

My transformation came after reading an article by nonviolent activist Dr. Khales Jalabi. In that article, he said that God gave us a mind so that we could think and could seek answers for everything – including for the existence of God Himself. At that moment all my fears vanished, and I became a completely different person. I wanted to read about everything, and I began turning every answer back into a question.

I was fascinated by Dr. Jalabi's denunciation of violence and his support for the use of nonviolent tactics for instituting change. It was my admiration for Dr. Jalabi and for others like him that brought me to MEMRI.

MEMRI's Democratization in the Arab and Muslim World Project, of which I am director, provides Arab and Muslim reformists with a platform from which they can reach out to their societies and to religious, political, and educational leaders while also providing Western policy makers with a solid basis for long-term strategic plans aimed at supporting this effort.

Today, I see many Muslims trapped in the same sense of conflict and paradox in which I myself was once trapped – especially young Muslims in all parts of the world, even here in the U.S. The difference today is that Muslims now have many, many more opportunities to access the writings and songs that were the source of my extremist ideas. They are readily available online at jihadist forums and websites. These are powerful magnets for Muslims, especially young Muslims, who are looking for answers.

Based on my own experience and research, I know that these jihadi websites and forums are very effective at recruiting Muslims to their cause of reviving the glory of Islam and the lost Islamic Caliphate. Along with other media in the Muslim world, they campaign intensively against the U.S. and the West – presenting both as the eternal enemies of the Muslims, as satanic force conspiring against the Muslims and against their most precious asset – their Islamic faith.

The Role of Jihadist Websites

Jihadist forums and websites have played a role in several recent terrorist acts in the U.S. Major Nidal Hasan, the sole suspect in the November 2009 Fort Hood shootings, allegedly found ideas and encouragement on jihadist websites offering advice and instructions for perpetrating deadly attacks. Faisal Shahzad, the failed Times Square bombing suspect, may have put together his car bomb following the detailed instructions available on the forums.

These websites also post information on power stations, nuclear plants, and other sensitive potential targets for devastating attacks, as well as manuals for building explosive belts and bombs using readily available materials. Al-Qaeda in the Arabian Peninsula publishes an online magazine called *Inspire;* its most recent issue included instructions for making a bomb in a home kitchen, and guidance in how to kill as many people as possible when carrying out attacks in public places. That issue also included an article in English by the American-Yemeni sheikh Anwar Al-Awlaki; in it, he asked Muslims in America, especially those serving in the military: "How can you be loyal to an administration that is waging war against Islam and the Muslims?"

Two examples from this week show the very real danger posed by these terrorist websites. A member of the Islamist forum Shumukh Al-Islam posted Google Earth images of the U.S. military base in Djibouti, saying that "a trusted source" had provided him with information about the base's exact location. The images, he said, were a gift for the Somali jihad group Al-Shabab Al-Mujahideen. Second, a post on Al-Shumukh called on motivated Muslims in the U.S. to carry out martyrdom operations, such as suicide bombings, and showed how to make a car bomb similar to that used by Faisal Shahzad at Times Square. As part of MEMRI's ongoing support to the U.S. government and military, this information was provided to all interested parties.

I have personally witnessed the powerful effect a media campaign can have on young minds. During my student years in Sudan there was an ongoing war being fought between the Muslim government and the Christian insurgents in the south. The government recruited thousands of students to fight the insurgents, among them many of my friends and teachers; some of them would later lose their lives in the fighting. One government recruitment effort was a jihadist TV series called "In the Arenas of Martyrdom," that aired on state-run TV every Friday night. This show documented jihad fighters imparting their love for jihad, discussing their courageous deeds, and telling of the miracles they had witnessed on the battlefield. I still remember how fascinated I – and hundreds of my fellow students and millions of viewers around the world – were fascinated by their stories: a story of a fighter whose body did not decay after he was killed; another from whose blood a perfume-like fragrance wafted; a third whom the Prophet Muhammad visited in a dream; a fourth who saw angels fighting alongside the *mujahideen*; and a fifth who became invisible to the enemies after he recited a verse from the Koran. How I wept as I listened to the testimonies of these young men – each of whom was designated a "martyr" – and how I longed to become one of them! [You can see many such examples of Arab governments inciting to jihad on the website of MEMRI's TV Monitor Project at www.memritv.org]

This particular TV series, produced by the Sudanese government at considerable cost, persuaded thousands to join the Popular Defense Forces in order to achieve one of two desirable goals: either victory or martyrdom for the sake of Allah. Some may not realize what it means to see and hear a young man committing his last testimony to video before embarking on a martyrdom operation. I know how powerful these testimonies are, and what they mean to each and every Muslim, especially the youth.

Just as the Sudanese government managed to "market" the war in the South to recruit thousands to join the jihad there, terror organizations, especially Al-Qaeda, are actively recruiting thousands through the Internet, and persuading them to support and join the jihad. The method and means are the same – and so are the results.

In fact, Al-Qaeda and other jihad organizations consider their online activity to be an integral part of their jihad, and invest tremendous resources in it. Online and media activities are referred to as *al-jihad al-i'lami* ("media jihad"). In one of his recordings, Al-Qaeda deputy leader Ayman Al-Zawahiri praised those who engage in online jihadist activity, saying: "To the knights of the jihadi media I say: May Allah reward you the best reward for you good job in serving Islam. You must know that you are [fighting] on a great front of Islam, and that the tyrants [of our time] are very disturbed by your efforts..."[1]

The Internet – Essential to the Global Jihad Movement

It is impossible to imagine the development of the global jihad movement and the ongoing terrorism (and not just in the U.S.) without the Internet. The Internet has catapulted this primitive and murderous ideology right into the 21st century. Imagine a caveman emerging from his cave with the latest and most sophisticated missile launcher mounted on his shoulder. This actually happened – and the Afghan jihad managed to defeat the Soviet Union.

The Internet is likewise a sophisticated weapon in the hands of the global jihad, with which it gravely threatens the West, particularly the U.S. It is so vital for the global jihad that it has become an area of jihad in and of itself – electronic jihad.

Islamists consider their online activity as an integral part of their jihad, and therefore invest tremendous material and other resources in it. In fact, online media or information activities are referred to as *al-jihad al-da'wi* ("propaganda jihad") or *al-jihad al-i'lami* ("media jihad"). This concept is based on the well-known Hadith of the Prophet Muhammad: "One who sees a wrong must correct it with his hand, and if he cannot, then with his tongue, and if he cannot, then in his heart, and this is the weakest level of faith.")

Islamist websites operate out of various countries, both Muslim and non-Muslim, and their target audience includes countries and communities all over the world. Accordingly, the websites come in various languages – from Arabic, Farsi, Urdu, and Turkish to Western languages such as English and French. These sites tend to be ephemeral – every day new ones appear and others close down, or are shut down.

The online jihad activity of Islamist organizations takes numerous forms. Hacking Western government and commercial websites is a way of waging economic and ideological warfare against those whom they designate as their enemies. Online military training for jihad fighters includes weaponry handbooks, battle tactics training, information on explosives, and more. For example, the military committee of Al-Qaeda in the Arabian Peninsula publishes an electronic military journal, *Mu'askar Al-Battar* (The Al-Battar Training Camp). Some websites offer entire courses on explosives manufacturing, and guides for making explosives and even homemade dirty bombs.

However, what Islamist organizations use the Internet for the most is spreading their messages and propaganda. They consider this effort to be vitally important, and pour considerable resources into it; it comprises the majority of such organizations' online activity.

Prominent terrorists play an active role in these organizations' online media activities. For example, the perpetrator of the December 2009 Khost CIA base bombing, Jordanian terrorist Humam Al-Balawi (Abu Dajana Al-Khorasani), was a writer and supervisor on the Al-Hesbah forum, which served as the main jihadist forum until it was shut down.

The Solution

Through our research of jihadi websites, we at MEMRI discovered something very interesting – so interesting that we wrote a series of reports on it. One major issue in these reports is that many jihadist websites are hosted by Internet Service Providers (ISPs) that are not aware of the content that they are hosting.[2] We also reported on anti-Muslim incitement on the Internet[3].

In order to fight the spread of extremism on the internet, in July 2007 we addressed Congress at an event titled "The Enemy Within: Where are the Islamist/Jihadist Websites Hosted and What Can Be Done About It." We suggested one way to begin dealing with the problem: notifying ISPs in the U.S. of just what it is that they host, in the hope they would voluntarily remove the sites. Two Members of Congress, Representatives Gary Ackerman (D-NY) and Mike Pence (R-IN), sponsored the bi-partisan event, and spoke about the important issue of Islamist websites and the threat they represent against America. Both Congressmen called on ISPs in the U.S. to stop working in the service of global jihad. In the two weeks following the event, 32 of the 50 ISP companies questioned removed the jihadi sites from on their servers.

As a result of the briefing's success, MEMRI founded its Civil Action for a Jihad-Free Internet initiative, whose stated purpose is to notify ISPs that some of the sites they host may be considered a threat to national security. To our way of thinking, the exposure itself is an effective measure against extremist websites.

The Civil Action for a Jihad-Free Internet committee is made up of current and former Members of Congress, administration officials, intelligence community officials, Nobel laureates, and others. The group's purpose is to notify Internet Service Providers of the content they are hosting; hopefully, the ISPs, in turn, will remove it out of concern for national security.

Opposition to the Civil Action for a Jihad-Free Internet came in several varieties. One argument concerned First Amendment rights – although wiping out Internet jihad actually has nothing to do with freedom of speech. The U.S. criminal code bars the provision of communications services to any designated terrorist organization. Opponents in government who thought that the criminal code did not apply in this case should have given the Supreme Court a chance to rule on the matter.

A second argument is that these websites are a source of valuable intelligence, and therefore should be permitted. This, however, is totally inaccurate; these websites are for ideological recruitment, but provide no actionable intelligence. This argument was put forward, not surprisingly, by contractors who make their living by keeping these sites going.

A third argument concerns the "impossibility" of dealing with the huge number of these websites – presumably, if they are shut down by ISPs in the U.S., they will reemerge hosted by other ISPs, under new names and new URLs. But this too is invalid. First, despite the large number of jihadist websites, forums and blogs, we believe that only a few hundred, and perhaps even fewer, are the actual fonts from which the incitement flows – and that the rest are just reposting their content. We believe that if we can stop those key jihadi websites from operating, the rest of them will dry up.

The Fight Against Online Jihad Today

Cooperation among states and regimes, whether Western democratic or non-Western non-democratic, has developed considerably in recent years. Non-Western and non-democratic regimes are no less threatened than the West by global jihad and local jihad movements, and they have a vested interest in fighting online jihad. In the event that any country refuses to cooperate with a U.S. campaign against online jihad, naming them and focusing on them and their support for terrorism will be an effective tactic.

Most importantly, the number of jihadist websites has decreased in recent years, including those that were once sources and propagators of incitement. Currently, the number of highly dangerous ones is less than 10. Our last investigation through our Jihad & Terrorism Threat Monitor found that a very few important jihadist sites are hosted in the U.S.

One reason for this decline is that despite the arguments about First Amendment rights and possible intelligence value, intelligence services have made headway against online jihad by shutting down sites, and in some cases taking them over completely.

Another reason for the decline is the rivalry and mutual suspicions among some leading jihadist websites.[4] In addition, Al-Qaeda itself has severely cut down on the number of accredited websites publishing its releases due to this suspicion and paranoia over who is trustworthy.[5]

It is important to mention that terrorist organizations are always on the lookout for other channels and media through which to propagate their recruitment drives, ideological message, propaganda, and ideology. As jihadists encountered increasing difficulties with their websites, they discovered that they could easily turn to Western social media outlets such as YouTube, Facebook, and Twitter. A group named the Internet Jihad Brigades Invasion is an example of such a group using this medium. Their mission is to transfer material to such social networking outlets when difficulties are encountered in posting it on jihadist websites and forums. YouTube is the primary clearinghouse for one of America's most wanted terrorists, Anwar Al-Awlaki. Al-Awlaki provided the spiritual guidance and inspiration for several recent successful and failed terror attacks in the U.S. Major Nidal Hasan, Umar Farooq Abdulmutallab, and Faisal Shahzad have all been shown to have had a connection to Awlaki. As of this writing, over 5,000 videos on YouTube are spreading Awlaki's message of jihad.[6]

Al-Awlaki's presence on YouTube is the result of the shutting down of his website in November 2009, shortly after the Fort Hood shooting. At that time, MEMRI reported that Al-Awlaki's website was hosted by an ISP in California; within two hours of the report's publication, the ISP removed Al-Awlaki's website.[7]

Online jihad is a dangerous foe; the U.S. must confront it exactly as it confronts other forms of extremism on other fronts around the world – both within and beyond its borders. As with its military ventures, in order for this effort to bear fruit, the U.S. must initiate cooperation with its allies and with international organizations.

Experience shows that this can indeed be done.

Mr. Chairman, this concludes my opening remarks. Thank you again for inviting me today. I welcome any questions that you or the Members may have.

*Please note that MEMRI's staff is always available to answer questions or assist Congress in any way needed.

[1] Rajab 1431 (June-July 2010). Produced by Al-Qaeda's media wing, Al-Sahab, and posted on jihadist websites July 19, 2010.

[2] See: MEMRI Special Report No. 31, "Islamist Websites and Their Hosts Part I: Islamist Terror Organizations," July 16, 2004, http://www.memri.org/report/en/0/0/0/0/0/0/1174.htm; MEMRI Special Report No. 35, "Islamist Websites and their Hosts Part II: Clerics," November 11, 2004, http://www.memri.org/report/en/0/0/0/0/0/0/1257.htm; MEMRI JTTM No. 374, "The Enemy Within: Where Are the Islamist/Jihadist Websites Hosted, and What Can Be Done About It?," July 19, 2007, http://www.memrijttm.org/content/en/report.htm?report=2300 .

[3] See MEMRI Inquiry and Analysis No. 385, "Islamophobia and Jihad on Video-Sharing Websites(1): Islamophobic Videos on YouTube," September 7, 2007, http://www.memri.org/report/en/0/0/0/0/0/0/2369.htm; MEMRI Inquiry and Analysis No. 417, "Burning The Koran on YouTube: Islamophobia on Video-Sharing Websites (II)," January 30, 2008, http://www.memri.org/report/en/0/0/0/0/0/0/2520.htm .

[4] See MEMRI Inquiry & Analysis No. 625, "Tension, Suspicion Among Jihadi Websites Following Infiltration, Collapse of Several Sites," July 14, 2010, http://www.memri.org/report/en/0/0/0/0/0/50/4449.htm; MEMRI JTTM No. 275, "Al-Tajdeed Versus Al-Hesbah: Islamist Websites & the Conflict Between Rival Arab & Muslim Political Forces," May 17, 2006, http://www.memrijttm.org/content/en/report.htm?report=1691&param=IDTA .

[5] See MEMRI Inquiry & Analysis No. 625 "Tension, Suspicion Among Jihadi Websites Following Infiltration, Collapse of Several Sites," July 14, 2010, http://www.memri.org/report/en/0/0/0/0/0/50/4449.htm .

[6] See MEMRI Inquiry and Analysis No. 576,"_Deleting Online Jihad and the Case of Anwar Al-Awlaki: Nearly Three Million Viewings of Al-Awlaki's YouTube Videos – Included Would-Be Christmas Airplane Bomber, Fort Hood Shooter, 7/7 London Bomber, and Would-Be Fort Dix Bombers," December 30, 2009, http://www.memri.org/report/en/0/0/0/0/0/0/3871.htm .

[7] See MEMRI Special Dispatch No. 2638, "U.S.-Born Yemen-Based Imam Anwar Al-Awlaki on His CA-Hosted Website: Fort Hood Shooter 'Nidal Hassan Is A Hero,'" November 9, 2009, http://www.memri.org/report/en/0/0/0/0/0/0/3776.htm .

Mr. SHERMAN. I want to thank you for that testimony and I believe your written testimony is longer and, without objection, will be made as a part of the record. I recommend to my colleagues the first illustrative paragraph of your written testimony.

Next I would like to introduce Christopher Boucek. He is an associate in the Carnegie Middle East Program where his research focuses on security challenges in the Arabian Gulf and North Africa. Please proceed.

STATEMENT OF CHRISTOPHER BOUCEK, PH.D., ASSOCIATE, MIDDLE EAST PROGRAM, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

Mr. BOUCEK. Mr. Chairman, Ranking Member, and distinguished members of the subcommittee, thank you very much for the opportunity to be here today to speak about this very important topic. I think I would like to keep my remarks relatively brief, as my written testimony has been entered into the record, so we can move on to questions that you may have.

As we all know and as was mentioned in the opening statements, the issue of Web sites promoting and propagating jihadist terrorist ideology is a serious concern. I think it is important that we keep in mind what the Internet does and how this plays with recruitment and radicalization. It serves as a system to propagate and perpetuate an ideology as well as provide ideological cohesion and a sense of belonging across great distances. It is an unrivaled source for connectivity for sharing information, as well as knowledge, inspiration, propaganda, recruitment, and fund-raising efforts.

What I would really like to do is focus on three aspects that I outlined in my written testimony.

The first is a need for measured response, which I think would fall somewhere between the polite versus safe setup that we heard in the opening remarks. I would propose that there is a need for a very strong and coordinated approach to dealing with these issues, and I think that has to come from a basis of understanding what these issues are all about and how the Internet is being used. There are times that I would say that certain Web sites should be shut down or named and shamed, as have been outlined.

I would also say that we need to weigh this against the unintended consequences that can arise from doing so. There is a value, a considerable value for keeping some of these Web sites available for law enforcement intelligence as well as research efforts. I think we also need to keep in mind that over the last several years a number of experts have pointed out how there is a decreasing value in both shutting these down and as using them for surveillance or research methods. So I think this issue has an awful lot of nuance in it.

I would like to pick up on a point that was made by the previous witness, which is the use of YouTube, especially the use of YouTube by al-Qaeda in the Arabian Peninsula. About 3 months ago, a new YouTube channel appeared branded as AQAP, the Islamist al-Qaeda organization based in Yemen, their media outlet. This features all of AQAP's videos subtitled into English.

No longer do you need to have access to Arabic. No longer do you need to be able to navigate Web forums. In conjunction with English language propaganda material, you can now use Google and YouTube to access this material, and it is everywhere. Taken in the case of Anwar al-Awlaki, his sermons and lectures are available widespread, not just on YouTube but on an infinite number of outlets.

It is important to keep in mind that shutting down these Web sites will not completely eliminate the sentiment behind them, and I think this leads me into my next point, which is the need for an increased sense of counter-engagement, I guess the read and talk aspect.

And I think what I would say here is that it is important, I think, for us to keep in mind that al-Qaeda is fueled by an ideology and a set of ideas and a set of grievances, and we need to understand these, and there are some individuals—there are multiple pathways to radicalization, and there are some individuals who are motivated through religion, who benefit from religious discussion. And there are a number of programs in other countries—Internet-based, radio-based, television-based interactive programs—to discuss these issues.

We don't need to do this all ourselves, and oftentimes we probably should not be, and there are ways in which I think we can support these programs in other countries. We can support moderate—moderate voices that speak out in the region against violence. This comes with a caveat that some of those voices that are speaking out against violence are probably also speaking out on issues that would be of great displeasure to a number of people in this country. So we need to weigh the balance of these issues.

The last point I would like to make is how we look forward on some suggestions, and this is why I would highlight need for research and further research. I guess this is no surprise coming from an academic and a researcher. I think, basically, I would say that it is unbelievable to me that almost 10 years into this struggle we have yet to fully set up a way to address dealing with these issues.

If you look 10 years into the Cold War, we had a much, much better developed understanding of the Soviet Union, China, communism, socialism, the Russian language, Chinese. We are nowhere near that dealing with this issue. Across military, universities, higher education, I mean, this is shocking to me and I think this is something that we need to fix straightaway.

I think we also need to keep in mind that the Internet is not always a perfect mirror for what is going on in the ground in a lot of these countries. I think it is very easy to use the Internet to try to understand what is going in places where most Americans don't go, if it is Peshawar or Marab or other places, but there is no replacement for actual on-the-ground field research and interaction with people.

With that, I would like to highlight several other points, and I think that there are ways that, because this is an argument based on ideology and ideas, we can highlight the flaws and the inherent discrepancies in these arguments. I think doing this in conjunction with the more rigorous shut-down approach is probably where I would say we should head forward.

With that, I would like to conclude my remarks. Thank you very much, and I look forward to your questions.

[The prepared statement of Mr. Boucek follows:]

CARNEGIE ENDOWMENT
FOR INTERNATIONAL PEACE

Congressional
Testimony

U.S. STRATEGY FOR COUNTERING JIHADIST WEBSITES

Testimony by Christopher Boucek
Associate, Carnegie Middle East Program
Carnegie Endowment for International Peace

House Committee on Foreign Affairs, Subcommittee on
Terrorism, Nonproliferation, and Trade
Washington, D.C.
September 29, 2010

Chairman Sherman and distinguished members of the Subcommittee:

As members of this Subcommittee are well aware, the issue of websites promoting and propagating jihadist ideology continues to be a major concern. In previous testimony I have highlighted the challenges presented by the internet in recruitment and radicalization. The ubiquity and global connectivity of the internet has proven to be an unrivaled source of knowledge and inspiration, as well as an unmatched vehicle for terrorist and extremist propaganda, recruitment, and fundraising.

The role of internet propaganda has received renewed attention following the rise in public prominence of Anwar al-Awlaki, the Yemeni-American cleric, and his alleged role in inciting English-speaking foreigners to engage in violence and militancy. Awlaki and his reported ties to several ongoing investigations have again highlighted the power of the internet to reach large and disparate audiences.

The challenge of how to best respond to jihadi websites requires careful consideration on several points.

The Need for a Measured Response

Inaction is not a viable option. There needs to be a strong and coordinated approach to understanding how and why the internet is used by extremists before we can begin to design appropriate strategies for addressing these different factors. I would suggest that, at times, there is justification in seeking to shut-down websites advocating violence. This approach is not one that I would quickly or broadly endorse, as there is considerable value for various law enforcement, intelligence, and research communities to continue to have access to these sites. But several experts have noted that the surveillance value has decreased somewhat over time as some internet users have grown more suspicions and paranoid about using the internet.

For instance, there is a YouTube channel branded by al-Malahim, the media arm of al-Qaeda in the Arabian Peninsula (AQAP), the resurgent al-Qaeda organization based in Yemen. This channel features almost all of AQAP's video messages, subtitled into English, including several messages from AQAP leaders, justifying terrorist attacks and railing against the Yemeni and other governments. It also includes at least one interview with Anwar al-Awlaki. As a result AQAP's message is able to reach a much broader audience, and no longer does someone need to know Arabic or need to bother with Islamist web forums to access this content. For almost three months this material has been available and not taken down. YouTube should remove this content.

However, we must be clear about the limitations of such strategies and we must also be realistic about what we can accomplish. Shutting down websites will not completely eliminate the sentiments behind them. The appeal of taking down such sites should also be weighed against all the potential unintended consequences, including driving users to other sites and social media outlets. For some users, the closing of certain sites may be enough to deter their continued online activism. For others it will not.

The Need to be Proactive, Not Just Reactive

In order to comprehensively fight extremist recruitment and radicalization, it is essential that we broaden our approach. To get ahead of al-Qaeda, and Islamist extremism more broadly, we will need to shift to be proactive, and not just reactive. We must engage on all levels, and that will involve not just counter-messaging, but challenging radical voices and narratives in a variety of forums.

On many levels, the struggle against violent radical Islamist extremist is about ideas, and unless we are active in meeting and challenging those ideas, we have all but surrendered this vital space. It is important to note that there are individuals who get involved in extremism out of a desire to "do right." Others get involved following an inability to distinguish between credible and non-credible sources of religious scholarship.

We have yet to truly understand how we can fully take advantage of the internet to highlight fractures and wedge issues among online extremists. This can complement efforts to "disaggregate" extremists in order to make the problem more manageable, rather than operating under the false presumption of a unified and cohesive opponent.

We do not need to do this all ourselves and in some instances it may be counterproductive to be engaged in such activities. There are many voices in the Arab and Muslim world that have spoken out against violence and extremism, some official and others not, some regime-supported and others at odds with their own governments. Some voices that challenge the use of violence may simultaneously also advocate other positions offensive to U.S. policymakers. In such cases it will be important to carefully weigh the consequences and differences between countering violence and promoting alternative values.

Other nations have explored a variety of methods to engage in counter-radicalization efforts. In Saudi Arabia, the Sakinah Campaign has shown promise. Named after the Arabic word for religiously inspired tranquility, the Sakinah Campaign operates as an independent, non-governmental organization, supported by the Ministry of Islamic Affairs. Similar to other counter-radicalization and disengagement strategies in the kingdom, the Sakinah Campaign uses Islamic scholars to interact online with individuals looking for religious knowledge with the aim of steering them away from extremist sources. The Sakinah Campaign was created to engage in an online dialogue as a way to combat internet radicalization. It targets individuals who use the internet to seek out religious knowledge and aims to prevent them from accepting extremist beliefs. It seeks to refute so-called "deviant' interpretations of Islam and rebut extremist arguments, including the ideology of takfir (the pronouncement that someone is an unbeliever and a key justification for violent extremism). While the campaign is supported and encouraged in its work by Saudi Arabia's Ministry of Islamic Affairs, Ministry of Education, and Ministry of Interior, it is officially a non-governmental project. There are in fact other governmental internet-based efforts to combat internet radicalization, although many of these programs are kept from public view in order to be effective. The independence of the Sakinah Campaign helps contribute to its relative legitimacy and results in more people being willing to work with them in their efforts to combat extremism online. Saudi authorities have noted that other countries have sought to create similar programs, including Kuwait, the United Arab Emirates, Algeria, the United Kingdom, and the United States.

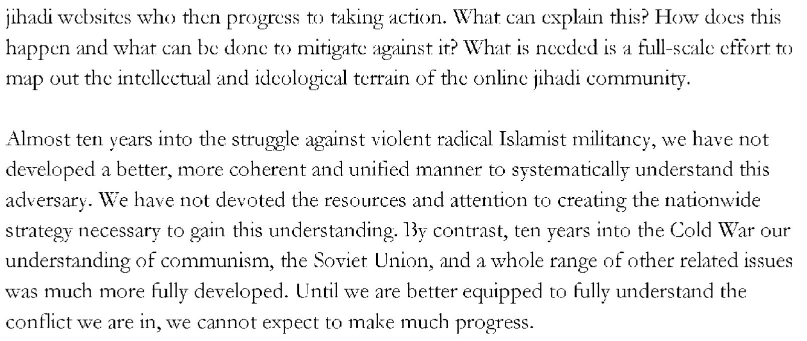
Other similar efforts have included endeavors such as Tunisia's Radio Zitouna. When it was started in 2007, Radio Zitouna was focused on broadcasting a 'tolerant' version of Islam and interpretation of the Holy Quran, including an educational call-in show. As of last year, station operators had plans to also start a television channel. Radio has also been used as a means to combat extremism in other cases in North Africa, the Sahel, and Middle East.

Looking Forward

In the struggle to combat extremism, much emphasis has been placed on the internet. While the internet no doubt has a role to play, it is important that we keep it the proper perspective. There is reasonable concern that the internet, when used as the sole lens through which extremism is viewed, can result in a distorted impression of what is actually happening on the ground. There can be no substitute for actual on the ground field research. Similarly, the internet should not be used as a replacement for examining other media and personal interactions as a means to counter radicalization.

A final crucial component that requires attention is the critical need for further research. There are many questions for which we simply do not have the answer and to comprehensively combat internet extremism it is essential to understand what we are trying to deal with exactly.

For instance, there are some individuals who are active online and violent in real life, some who are active online but do not engage in violent actions, and still others who are active on



jihadi websites who then progress to taking action. What can explain this? How does this happen and what can be done to mitigate against it? What is needed is a full-scale effort to map out the intellectual and ideological terrain of the online jihadi community.

Almost ten years into the struggle against violent radical Islamist militancy, we have not developed a better, more coherent and unified manner to systematically understand this adversary. We have not devoted the resources and attention to creating the nationwide strategy necessary to gain this understanding. By contrast, ten years into the Cold War our understanding of communism, the Soviet Union, and a whole range of other related issues was much more fully developed. Until we are better equipped to fully understand the conflict we are in, we cannot expect to make much progress.

Mr. SHERMAN. We will now hear from our third witness, Mr. Gregory McNeal. Mr. McNeal is an associate professor of law at Pepperdine University School of Law located immediately adjacent to the 27th Congressional District and previously found in the 24th Congressional District of California. He has also served in an advisory capacity on counterterrorism policy to the Departments of Defense and Justice.

Mr. McNeal.

STATEMENT OF GREGORY S. MCNEAL, J.D., ASSOCIATE PROFESSOR OF LAW, PEPPERDINE UNIVERSITY

Mr. MCNEAL. Chairman Sherman, Ranking Member Royce, distinguished members of the subcommittee, it is an honor to be here today to speak about the threat of terrorist Web sites and the U.S. strategy to counter them.

As a professor at Pepperdine University, I specialize in national security law and policy, and I have written specifically about the threat of terrorist Web sites.

As a California resident, it is an honor to be here speaking before the subcommittee, which has been so ably led by California representatives, Congressmen Sherman and Royce.

In the era of home-grown terrorist plots, terrorist Web sites are a grave threat to national security, which require a three-pronged approach to combating them. That approach combines monitoring for intelligence value, elimination and destruction for operational gains, and co-optation for propaganda and ideological value. My remarks today and my written testimony focus on the elimination and destruction of terrorist Web sites.

Eliminating selected extremist Web sites will enhance our ability to collect intelligence by narrowing the field of enemy sites we must monitor. A small number of Web sites will allow for target efforts to undermine the jihadist message. Finally, efforts which keep the enemy on the move impose costs on them. They delegitimize them and at the margins make it more difficult for potential recruits to become radicalized.

Today's headlines about a plot to engage in coordinated Mumbai-style terrorist attacks reveals the critical importance of countering the terrorist Web presence. Home-grown, low-sophistication, high-casualty plots are increasingly facilitated by jihadist Web sites.

Consider just a handful of our close calls here within the United States.

Nidal Hasan, the Fort Hood attacker, was inspired by and radicalized by terrorist Web sites. Those Web sites now hold him up as a symbol of successful, home-grown attacks.

Najibullah Zazi, who planned a second series of attacks against the New York City subway system, was radicalized and educated through jihadist Web sites.

Faisal Shahzad, the Times Square bomber, was radicalized through terrorist Web sites. It was there that he found his inspiration and fixity of purpose that drove him to carry out his attack.

Internet images of jihad were the singular tie binding together the efforts of the Fort Dix plotters. And, moreover, in the case of Ohio terrorists Mohammad Amawi, Marwan El-Hindi and Wassam Mazloum, terrorist Web sites were the motivating and enabling factor in the recruitment, providing them with information about how to build bombs.

The common theme running throughout nearly every attempted attack since September 11 is a radical ideology. That ideology finds its home in a small core of Web sites with close operational ties to al-Qaeda. Those core forums are the mainstream media of extremist ideology. They have the label of legitimacy. Their stories, videos, training materials, and directives are picked up by mirror sites and repeated throughout the Web. We should be disrupting their operations.

I would like to address a common myth that shutting down terrorist Web sites does not work. I say this is a myth because, to date, there has been no concerted government effort to shut down these sites. I readily admit that the terrorist Web presence cannot be eliminated, but that is not the goal of what I am advocating for. Rather, the goal I believe we should be pursuing is to impose costs on our enemies in time and resources to narrow their potential Web hosts and corral them into places of our choosing so we can monitor and co-op them. It should not be easy for our enemies to recruit, train, and proselytize.

The Internet is not a battlefield that should operate according to the directives of our enemies. Rather, it is a battle space that we should own. On the traditional battlefield, few would argue that we should forego killing and capturing terrorists merely because they may be quickly replaced. Yet when it comes to the Internet that is exactly what those who are opposed to shutting down these Web sites are advocating for. Now, I am speaking in terms of warfare.

However, the fight against terrorist Web sites must be an interagency effort. The intelligence community, the military, law enforcement, and the State Department are all key players in a comprehensive strategy to counter the threat of jihadist Web sites. However, this should not be solely the province of the executive branch. In fact, I believe that comprehensive legislation directing and prescribing the activities of each agency in the cyber realm is essential to national security.

Congress can and should make its mark before the executive branch takes actions on its own, forming precedent without policy.

The threat of jihadist Web sites is one part of a broader need for legislation directing of our Nation's cyber war efforts. The key to countering the influence of terrorist Web sites is to first ensure that those Web sites do not receive any support from U.S. Web hosts. This can be accomplished through application of existing laws and shaming techniques. Second, we should eliminate selected sites using existing statutes and Treasury regulations. Third, we should work with allies to target those individuals who are supporting Web sites abroad that are beyond the reach of our law. And, finally, when necessary, actions should be taken by the Pentagon's Joint Functional Component Command Network-Warfare Unit and Cyber Command to shut down selected Web sites. However, this should only be done after coordination and consultation with the intelligence, law enforcement, and diplomatic community; and Congress should be regularly informed of these actions. Following these steps will go a long way toward countering the influence of jihadist Web sites.

This concludes my formal remarks.

[The prepared statement of Mr. McNeal follows:]

"U.S. Strategy for Countering Jihadist Websites"

Testimony by Gregory S. McNeal
Associate Professor of Law
Pepperdine University School of Law

Before the

United States House of Representatives
Committee on Foreign Affairs
Subcommittee on Terrorism, Nonproliferation and Trade
September 29, 2010

PEPPERDINE UNIVERSITY
School of Law

Terrorists are engaged in an online jihad, characterized by the use of the Internet to fundraise, distribute messages and directives, recruit, and proselytize. Although it is impossible to eliminate the presence of terrorists on the Internet, and in some instances imprudent, my testimony details a series of proposals that can have an impact on the presence of terrorists on the Internet. Using existing statutes and watchdog groups, it is possible to regionalize terrorist Web sites, limiting them to a small number of countries from which they may receive Internet services. Once the terrorist message is limited to a particular region, a modification of current laws can allow a cyber embargo on jihadist Web sites and their supporters. These efforts, coupled with diplomatic cooperation, can further the attempt to curb the impact of jihadist Web sites, while simultaneously increasing the ability of governments to monitor these Web sites and, when necessary, shut them down.

As others have noted in testimony and policy articles, terrorist Web sites may move their operations and continually pop up at new hosts, especially given the dynamic nature of the Web. However, like other battlefields in the struggle against terrorist organizations, efforts that keep the terrorists moving impose costs on their operations. These costs include preventing the distribution of the terrorist message, disrupting the organization's regular activities, and damaging the morale of the organization.[1] Efforts to counter the terrorist presence on the Web can force such organizations to overseas Internet service providers (ISPs), thus limiting their host options and increasing the likelihood that authorities will be able to track them and monitor them.

Step one in the process of shutting down a terrorist Web site is to use shaming techniques and the threat of criminal sanctions to stop US companies from providing services to designated terrorist organizations.[2] As an example, Web sites such as Internet Haganah posted the details of US companies that were providing services to Palestinian Islamic Jihad (PIJ) as part of a shaming campaign. The Web site encouraged readers to contact those US companies and demand that they stop supporting terrorists. The US companies have more at stake than just their reputations. Current statutes make it a crime to provide material support to terrorist organizations, and the list of prohibited forms of support includes the provision of computer services. Shortly after the shaming campaign, with its attendant potential for criminal liability, the PIJ Web site shifted its operation to overseas Internet service providers (ISPs) that are beyond the reach of US laws and less susceptible to shaming techniques. As a result, while temporarily troubled by their exposure, the PIJ Web site is still operating today.

Thus, the second step to further isolate and eventually shut down terrorist Web sites is the most critical one. Current laws and techniques are limited, and terrorist organizations are quick to adapt and avoid the reach of shaming techniques and US laws. Nevertheless, once terrorist organizations make their home outside the United States, they must still rely on the support of ISPs in their new jurisdictions. While the terrorist organization itself may not be deterred by US efforts, their ISPs are vulnerable to commercial pressure and the desire to maintain their business, the majority of which likely comes from non-terrorist clientele. These ISPs are the critical and weakest link in the terrorist's Web presence. Accordingly, a cyber embargo is the quickest and most effective way to cease their support of terrorist organizations. Such an embargo focuses on those ISPs that are providing material support to terrorist Web sites in the form of Web services.

[1] Boaz Ganor, The Counterterrorism Puzzle 102 (2005).

[2] The U.S. State Department and Department of Treasury both maintain lists of designated terrorist organizations. Those lists are available at http://www.state.gov/s/ct/list/index.htm and http://www.treas.gov/offices/enforcement/ofac/sdn/ respectively.

This is true because, after being forced off of US network service providers, a terrorist Web site will need to receive an IP address and connection to the Internet from overseas providers. I propose a modification to existing statutes to create a new cyber supporter designation that will sweep these ISPs within the sanction of US laws. Under this approach, US companies and persons will be forbidden from doing business with a designated cyber supporter. The practical result of such a designation will be to create a cyber embargo, cutting off streams of income to overseas companies due to their affiliation with terrorist organizations.

With a cyber embargo in place, companies that support terrorists will be forced to choose between losing all commercial services from the United States and continuing to provide services to the terrorist organization. The result is obvious; if the terrorist's ISP was a major international telecommunications company and it was designated as a cyber supporter, then all US commercial services would be cut off, including Internet and financial services. In the face of such potential loss of income, that company would likely cease providing services to the designated terrorist group. Nevertheless, it is still possible that the overseas company may not be deterred by a cyber-supporter designation. As such, a further step is necessary to isolate these terrorist organizations and their overseas Web hosts. The third step involves diplomatic efforts to standardize the creation of "designated cyber supporter" lists by urging nations to adopt the list and implement necessary domestic enforcement mechanisms. Such an adoption will expand the number of nations participating in a cyber embargo and will foreclose overseas safe havens for terrorist Web sites. Expanding the cyber embargo is key because, as an overseas terrorist Web site continues to shift its operations to countries that it believes are safe havens, the cyber embargo will continue to isolate them geographically. This type of cooperative diplomatic approach is one which has been particularly successful in Europe through the "Check the Web" initiative an open-source monitoring and database creation project handled by the European Law Enforcement Organization (Europol), for the purposes of monitoring the Internet for terrorist use, especially recruitment, training, and propaganda.

TREASURY REGULATIONS AND IEEPA AS A POTENTIAL TOOL

The Treasury Department has an underused tool allowing for broad sanctioning authority that also can be used against terrorist Web sites. This authority was created by the International Emergency Economic Powers Act (IEEPA).[3] The Treasury's authority to confront and counter terrorists in cyberspace stems largely from the powers provided to the President by IEEPA. The IEEPA allows the President to declare a national emergency in response to a threat to national security, foreign policy, or the economy of the United States. With such a declaration, the President can exercise a broad set of powers, including blocking property, investigating, and regulating and prohibiting transactions.[4] On September 23, 2001, President Bush invoked this power, declaring a national emergency with respect to the threat posed by al-Qaida, and issued Executive Order 13,224, "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism."[5]

[3] 50 U.S.C. §§ 1701-1707 (2000).

[4] *Id.* §§ 1701-1702 at 232, 253, & 262.

[5] Exec. Order No. 13,224, 3 C.F.R. § 786 (2001), *reprinted in* 50 U.S.C. § 1701 (Supp. III 2000).

The order included an initial list of 27 targets, including Osama bin Laden and al-Qaida.[6] In addition, it provided that the Secretaries of State and Treasury could add specified categories of persons (individuals and entities) to the list.[7] The categories of individuals and entities eligible for designation by the Secretary of the Treasury are:

> (a) persons determined to be owned or controlled by, or to act for, or on behalf of, those persons either listed in the Annex to the EO [Executive Order] or determined to be subject to the EO;
> (b) persons determined to assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, those persons listed in the Annex to this order or determined to be subject to this order;
> (c) persons determined to assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, acts of terrorism as defined by the EO, or
> (d) persons determined to be otherwise associated with those persons listed in the Annex to the EO order or those persons determined to be subject to the EO.[8]

Placement on the list requires US persons, which for purposes of this testimony would include ISPs and domain name registrars, to block property and interests in property, including "services of any nature whatsoever,"[9] belonging to the designated sanctions targets.[10] In addition, US persons are prohibited under EO 13,224 (and its implementing regulations) from engaging in "any transaction or dealing . . . in [blocked] property or interests in property," including the provision of services to or for the benefit of persons designated pursuant to the EO.[11]

This means that Treasury Regulations may be an extremely effective tool in countering the Internet jihad. Those companies organized under the laws of the United States, or any ISPs physically located in the United States, are thus prohibited by law from providing Internet service to or for the benefit of al-Qaida, Hezbollah, Hamas, PIJ, and any other entities or individuals designated pursuant to the EO.

Furthermore, treasury regulations found in 31 C.F.R. § 594[12] area source of potential sanctions for ISP's supporting jihadist Web sites. According to OFAC guidance, those who wish to provide services to targets of Treasury sanctions may not do so without *ex ante* case-by-case

[6] *Id.* at 790.
[7] *See id.* at §1.
[8] *See id.* §§ 1(c), (d)(i).
[9] 31 C.F.R. § 594.309 (2006).
[10] 31 C.F.R. § 594.301.
[11] 31 C.F. R. § 594.406.
[12] US Dep't of the Treasury, Office of Foreign Assets Control: Mission, *http://www.treas.gov/offices/enforcement/ofac/*.

authorization by Treasury.[13] The potential civil penalty for violations of IEEPA regulations is $250,000.[14]

Acting pursuant to these authorities, the Treasury may issue cease-and-desist orders (C&Ds) to US-based ISPs providing services in violation of existing sanctions programs. OFAC investigators often serve C&Ds on US persons involved with a designated target.[15] The C&Ds would be issued pursuant to IEEPA, EO 13,224 (or possibly EO 13,438),[16] and 31 C.F.R. § 594. If systematically employed as part of a long-term program targeting terrorist Web sites, jihadists will be forced to seek domain names and ISPs from overseas hosts.

Under the same laws and regulations, OFAC can also demand information from ISPs' client lists, such as those clients receiving domain names or Web-hosting. These administrative subpoenas—known as 602s after the relevant section of the regulations—are another traditional OFAC function.[17] Signing up for an account with an ISP generally involves providing your name, address, telephone number, and billing information, which invariably includes a credit card number, placing terrorist Web sites squarely within the sights of 602s.[18]

While terrorists using the Internet are unlikely to provide accurate information and will likely employ stolen credits cards to make online purchases for their Internet services, existing Treasury regulations using 602s and C&Ds require little additional effort and may produce valuable leads. The example of Irhabi007 supports this; investigators there found stolen credit card information and confirmed that the cards were used to pay US Internet providers on whose servers Irhabi007 had posted jihadi propaganda.[19] According to the *Washington Post*, that lead demonstrated to authorities that "they had netted the infamous hacker."[20]

SHAMING AND WATCHDOG GROUPS

Despite the fact that designated foreign terrorist organizations (FTOs) are publicly listed on the Department of State and Department of Treasury Web sites, Internet companies are oftentimes either undeterred by the threat of prosecution or are unaware of their client's terrorist status. As such, these companies frequently continue to do business with designated FTOs.

While the government has a legitimate interest in keeping terrorists from recruiting, it does not want to be seen as attempting to censor the internet. Thus, a wiser interim policy is to persuade Internet service providers and domain name registrars to voluntarily take down or suspend services when those services are assisting terrorist organizations. Network Solutions, a Virginia based company, for example, often avoids acknowledging the fact that it has retained, through its user policy agreement, the ability to regulate and take down a site that it deems "unlawful," "threatening," or which "constitutes an illegal threat, hate propaganda, profane, indecent or otherwise

[13] *See* O.F.A.C. Guidance Ltr., 030606-FACRL-IA-07 (June 3, 2003) (providing interpretative guidance on Iranian Transaction Regulation, 31 C.F.R. § 560, on the provision of Internet Connectivity Services and is persuasive with regard to the interpretation of Global Terrorism Sanctions Regulations).

[14] Press Release, Dep't of the Treasury, Office of Foreign Assets Control, Civil Penalties—Interim Policy (Nov. 27, 2007), available at *www.treas.gov/offices/enforcement/ofac/civpen/penalties/interim_pol_11272007.pdf.*

[15] *See* Statement by Assistant Sec'y Juan Zarate Before the UN Sec. Council 1267 Sanctions Comm., JS-2189 (Jan. 10, 2005), available at *http://treas.gov/press/releases/js2189.htm.*

[16] *See* Exec. Order No. 13,438, 27 *Fed. Reg.* 39,719 (Jul. 19, 2007), available at *http://www.treas.gov/offices/enforcement/ofac/legal/eo/13438.pdf.*

[17] 31 C.F.R. § 501.602.

[18] John R. Levine, *et al.*, The Internet for Dummies 60 (7th ed. 2000).

[19] Rita Katz & Michael Kern, "Terrorist 007, Exposed," *Wash. Post*, Mar. 26, 2006, at B1.

[20] *Id.*

objectionable material of any kind or nature."[21] Of course, Network Solutions is not the only Web service provider that hosts extremist Web sites. For example, another site based in Dallas, *thePlanet.com*, was accused of hosting three different terrorist Web sites and a Hamas monthly news magazine, each run by designated FTOs.[22]

Because it is difficult for companies and the government to monitor to whom Internet services are being provided, independent watchdog sites stand in the best position to fill the gap. A number of watchdog sites already monitor the Internet for terrorist activity and information. This brings me back to the example of Internet Haganah. While Internet Haganah is primarily run by Weisburd out of his home, it enjoys the help of groups from around the world.[23] After finding a terrorist Web site, Weisburd determines which Internet companies are providing the site support and either "shames service providers into shutting down the sites that host them or gathers what he terms 'intel' for interested parties."[24] These interested parties include both government and private entities.[25] Internet Haganah encourages individuals to take action by learning about both the terrorist Web site and the group, understanding the terms of service of the host company, and finally making a calm, informed, complaint to the company.[26] Often these complaints go unanswered, at which point Internet Haganah recommends that an individual go to the local media for publicity.[27] No company wants to see its name smeared across the morning news as a supporter of terrorism, especially in their key market.[28]

Tactics such as these have successfully encouraged sites to take down other questionable material, such as Web sites that cater to pedophiles. For example, in April 2007, Network Solutions shut down a Web site after receiving complaints from customers.[29] The site had been publicly broadcast in The Bellingham Herald newspaper, prompting the complaints.[30] Company spokeswoman Susan Wade responded by saying that, although there is no way that Network Solutions could possibly "police the content of everything that's going up because hosting providers can sell thousands of sites a day," it appreciates when third parties get involved or "when we get served legal papers that say, 'Hey, take a look at this.'"[31]

OTHER LEGAL ACTION AND ASSOCIATED CHALLENGES

When shaming, complaints, and bad publicity fail, government officials may need to bring legal action against companies that are providing support to terrorist organizations. The US Senate Committee on Homeland Security and Governmental Affairs has conducted hearings on violent Islamic extremism, covering various aspects of the problems, including how the Internet fosters

[21] Network Solutions Acceptable Use Policy, *http://www.networksolutions.com/legal/aup.jsp.*

[22] "Dallas Server Company Carries Zarqawi Death Videos, Terrorist Websites" (CBS-11 television broadcast Nov. 14, 2004), available at *http://haganah.org.il/hmedia/press-15nov04-cbs11-dallas.pdf.*

[23] Nadya Labi, "Jihad 2.0," *The Atlantic Monthly*, Jul./Aug. 2006, available at *http://www.theatlantic.com/doc/prem/200607/online-jihad.*

[24] *Id.*

[25] *Id.*

[26] *See* "Confronting the Global Jihad Online: What Can You Do," *Internet Haganah*, Nov. 18, 2004, *http://internet-haganah.com/harchives/003133.html.*

[27] *Id.*

[28] *See id.*

[29] *See* "Network Solutions Shuts Down Pedophile Website," *HostSearch*, Apr. 7, 2007, *www.hostsearch.com/news/network_solutions_news_5782.asp.*

[30] *Id.*

[31] *Id.*

recruitment and propaganda dissemination.[32] At the hearings, the George Washington University Homeland Security Policy Institute endorsed the use of "[l]egal means for disrupting extremist use of the Internet[, which] may be useful against websites that directly advocate violence or provide material support to known terrorist organizations, crossing the line from protected speech to illegal acts of violence."[33] The House of Representatives took notice of the presence of terrorism on the Internet and called on all corporate owners of Web sites that share user-posted videos to take down terrorist and jihadist propaganda.[34] Yet, even without this express resolution, the government already has a powerful legal tool available in the form of § 2339, the material support statute.

Prosecutors can use § 2339 to stop US Internet service providers (ISPs) from providing their services as "material support" to FTOs. Ignoring the threat of prosecution exposes companies to prison, fines, and significant public outcry. Section 2339 and its subsections holds that, if a person is found to have materially supported a designated FTO, that person "shall be fined under this title or imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life."[35] While to date no case has been brought against an ISP, a plain reading of the statute suggests that those who continue to provide services to terrorist Web sites after being notified of the sites support of terrorism have arguably satisfied the definition of providing "material support."[36] This is especially the case in light of the Supreme Court's recent opinion in *Holder v. Humanitarian Law Project*, which held that, providing a service to a terrorist organization is distinguishable from independent advocacy which is protected by the First Amendment.

While most prosecutions under § 2339 have centered on individuals who have physically provided material support, either through the provision of objects such as weaponry or funding, the statute has recently been used to prosecute individuals who use computers and the Internet as a means of providing material support.[37] In 2004, The District Court in Connecticut indicted Babar Ahmad on terrorism charges, including a violation of § 2339A, providing material support.[38] The charges allege that Ahmad created Web sites in order to "recruit mujahideen, raise funds for violent jihad, recruit personnel . . . solicit military items," and to give instructions on how to travel to Pakistan to fight for the Taliban and for the "surreptitious transfer of funds" to terrorist groups.[39] Some of the Web sites opened and maintained by Ahmad were serviced through a US company, OLM, which was headquartered in Connecticut at the time.[40]

[32] The Internet: A Portal to Violent Islamic Fundamentalism Before the S. Comm. on Homeland Security and Governmental Affairs, 110th Cong. (2007), available at *http://www.senate.gov/~govt-aff/index.cfm?Fuseaction=Hearings.Detail&HearingID=441*.

[33] The George Washington Univ. Homeland Sec. Policy Inst. et al., NETworked Radicalization: A Counter-Strategy 20 (2007), available at *http://www.gwumc.edu/hspi/reports/NETworked%20Radicalization_A%20Counter%20Strategy.pdf*.

[34] H.R. Res. 224. 110th Cong. (2007).

[35] 18 U.S.C. § 2339B(a)(1) (Supp.).

[36] *See id.*

[37] *See, e.g.*, Criminal Complaint at 3-4, United States v. Lindh, No. 02-51-M (E.D. Va. 2002) (claiming that John Walker Lindh admitted to traveling to Pakistan to receive paramilitary training and traveling to Afghanistan to join the Taliban); Indictment at 86-94, United States v. Al-Arian, No. 8:03-CR (M.D. Fla. 2003) (charging Sami Amin Al-Arian with conspiracy to provide material support to Palestinian Islamic Jihad-Shiqaqi by raising funds for the organization); Indictment at 10-20, United States v. Sattar, No. 02-Crim.-395 (S.D.N.Y. 2002) (charging Ahmed Abdel Sattar with conspiracy to provide material support to Islamic Gama'at by providing telephone equipment, financing, and transportation); Indictment at 7-9, United States v. Babar Ahmed, (D. Conn. 2004) (charging Babar Ahmed with conspiracy to provide material support to Al-Qaida by maintaining Internet accounts used to recruit members, solicit donations, and communicate to a US Naval enlistee encouraging "the enlistee to 'keep up the psychological warefare.[sic]'").

[38] Indictment at ¶ 18, United States v. Babar Ahmed (D. Conn. 2004)

[39] *Id.* at ¶ 12.

[40] *Id.* at ¶ 21A.

The Ahmad case proves that a material support prosecution for providing Internet services is at least conceivable; yet, no such actions have been brought against ISPs. This is likely due to the fact that most companies want to cooperate, and when they are reluctant to do so, their reluctance is short-lived when faced with the threat of prosecution.

Despite the utility of threatening prosecution, there are constitutional challenges to successfully using the material support statute. Some may argue that targeting ISPs amounts to censorship by proxy.[41] It is true that the "material support" statutes, or other similar criminal prohibitions that might be adopted, may "threaten to recruit a federally conscripted corps of censors...[and that] a risk-averse Internet intermediary would not need to descend into paranoia to conclude that the most prudent course would be to proactively censor messages or links that might prove problematic, and to respond to official "requests" with alacrity.[42] However, protecting individuals from innocent mistakes is why I argued that the first step in any enforcement strategy should be, as some watchdog groups advocate, to contact the ISP then to conduct a public shaming and media campaign. Only when those methods fail should the government consider prosecuting those companies who support terrorist Web sites. It is only then that the government can argue that the company was aware or "on notice" of its support of terrorist organizations. It is critical to bear in mind that the government in such a prosecution is not targeting the company's speech; it is instead targeting the company's provision of services to a designated terrorist organization. As the Supreme Court held this summer in *Holder v. Humanitarian Law Project*, providing a service especially when one is on notice that they are coordinating that provision of a service to a terrorist organization is a crime that is unprotected by the First Amendment.

BARRIERS TO USE OF TREASURY REGULATIONS

It is important to note that, Treasury regulations have faced First Amendment scrutiny and survived. For example, an examination of case law involving the constitutionality of OFAC actions involving First Amendment claims by US persons indicates that courts overwhelmingly rule in favor of the agency, especially when the cases involve counterterrorism-related enforcement actions. As stated in a D.C. Circuit Court decision, "there is no First Amendment right nor any other constitutional right to support terrorists."[43] Despite this fact, Treasury has not aggressively attempted to cut off cyber-services to terrorism supporters, not even to key al-Qaida facilitators.

Granted, there are some examples of attempted action, such as the December 2006 designation of Kuwaiti Hamid al-Ali, a cleric who supported al-Qaeda in Iraq and funded terrorist cells in Kuwait.[44] At the time of Hamid al-Ali's designation, the Treasury, under Secretary Stuart Levey, declared that these "individuals support every stage of the terrorist life-cycle, from financing terrorist groups and activity, to facilitating deadly attacks, and inciting others to join campaigns of violence and hate. The civilized world must stand united in isolating these terrorists"[45] Rather than isolating these terrorists, however, Hamid al-Ali continued to operate his Web site outside of Washington state.[46] His operations included the religious sanctioning of suicide bombings and the

[41] *See, e.g.,* Seth F. Kreimer, "Censorship by Proxy: the First Amendment, Internet Intermediaries, and the Problem of the Weakest Link," 155 *U. Pa. L. Rev.* 11, 11 (2006).
[42] *Id.* at 93-94.
[43] Holy Land Found. for Relief & Dev. v. Ashcroft, 333 F.3d 156, 166 (D.C. Cir. 2003); *see also* Humanitarian Law Project v. Reno, 205 F.3d 1130, 1133 ("[T]here is no constitutional right to facilitate terrorism[with materials or funding.]").
[44] Press Release HP-191, US Dep't of the Treasury, Treasury Designations Target Terrorist Facilitators (Dec. 7, 2006), available at *http://www.treas.gov/press/releases/hp191.htm.*
[45] *Id.*
[46] Chris Heffelfinger, "Kuwaiti Cleric Hamid al-Ali: The Bridge Between Ideology and Action," 5 *Terrorism Monitor* 4 (Jamestown Found., Apr. 2007), available at *http://www.jamestown.org/terrorism/news/article.php?articleid=2373349.*

incitement of individuals to "join the armed resistance of the jihadi movement[.]"[47] While Hamid al-Ali has reportedly renounced jihad, as recently as Monday, September 27, 2010 I was able to find this passage on his website, automatically translated from the original Arabic by Google:

> Simmer to the Islamic nation, to produce a comprehensive jihad to defeat the final this attack on our nation Alziosaliip, and purify the land of Islam from Rjsha, and expelled the Zionist entity from our country, and abort all plans, and restore the Islamic caliphate. Thank God that our nation great list to confront this challenge, the intention is stronger than the determination of black, and steadily like the stability of ancestors, and here made martyrs in every moment, across the front line that extends from the occupied Kashmir to Palestine beloved, through Afghanistan, the proud, and Iraq tall, to draw blood through the Glory , the path of sacrifice and send a brilliant victory, God willing.[48]

Ali's website receives registration services from Whois Manager out of Portland, OR; registrar services from Active Registrar, Inc., and servers from EuroVPS a UK based internet company. Ali is still preaching jihad, and he's doing so with the support of U.S. and allied companies.

In light of this, it's possible that the barriers Treasury action may be found, not in the First Amendment but in decades-old pieces of legislation. In 1988, Representative Howard Berman (D-Cal.) proposed the Berman Amendment, which limited the President's powers under IEEPA by creating an exemption for "informational materials."[49] Also, in 1994 Congress passed the Free Trade in Ideas Amendment, which expanded the Berman Amendment to non-tangible forms of information.[50] The Conference Report on the bill stated that the language of the Berman Amendment was explicitly intended to have broad scope.[51]

Given the age of these pieces of legislation, a case can be made that their silence regarding terrorism and Internet services supporting terrorism may provide for an exception to their broad scope. Even in the absence of an exception, one may argue that terrorist Web sites provide more than information, that is, by allowing fundraising, training, recruiting, and operational details, these Web sites provide "instrumental uses" that are distinguishable from "communicative uses."[52]

Moreover, in *United States v. O'Brien,*[53] the Supreme Court declared that government actions that advance "sufficiently important governmental interests" may allow incidental limitations on the First Amendment for speech and non-speech. The *O'Brien* court held that

> a government regulation is sufficiently justified if it is within the Constitutional power of the Government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on the alleged First

[47] *Id.*

[48] Webpage of Hamid al-Ali, http://h-alali.net/

[49] *See* The Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, 102 Stat. 1107 (1988) (codified at 50 U.S.C. § 5(b)(4)) [hereinafter Berman Amendment].

[50] Foreign Relations Authorization Act of 1994, Pub. L. No. 103-236, § 525; *see also* Berman Amendment.

[51] *Id.* (citing H.R. Rep. No. 103-482, at 483 (1994) (Conf. Rep.).

[52] *See generally* Gabriel Weimann, "www.terror.net: How Modem Terrorism Uses the Internet," 116 2004 *Inst. of Peace Special Report* 116 (2004), available at *http://www.usip.org/pubs/specialreports/sr116.pdf* (explaining many ways terrorist groups use the Internet, including training purposes).

[53] United States v. O'Brien, 391 U.S. 367 (1968).

> Amendment freedoms is no greater than is essential to the furtherance of that interest.[54]

Federal courts applying this test to OFAC activity have allowed the Treasury to restrict the import of books from sanctioned nations.[55] Courts have also upheld presidential action on the ground that barring provision of financial support to terrorists was unrelated to suppression of free expression and that any incidental restrictions on First Amendment freedoms were "no greater than necessary."[56]

Finally, Supreme Court precedent buttresses the view that not all speech in these contexts is protected. For example, speech that is likely to incite violence[57] or that creates a clear-and-present danger of a substantive evil[58] is unprotected. The content-neutral nature of statutes, regulations, and other government activity that can counter the cyber jihad makes a successful First Amendment challenge less likely. Accordingly, more government action against terrorist Web sites and their supporters is necessary to counter the cyber jihad and to fully define the limits of the First Amendment in this critical area of government concern.

A CYBER EMBARGO OF DESIGNATED MATERIAL SUPPORTERS

Even if the use of shaming and the threat of the material support statute or Treasury regulations can be successful in driving jihadist Web sites from US-based ISPs, the jihadist Web presence will still remain. As discussed already, a terrorist organization may maintain its Web presence by using the services of foreign companies. These companies are, in essence, providing material support, although they have not yet been charged or convicted of the specific offense. Thus, merely forcing jihadist Web sites overseas is not a sufficient counterterrorism strategy given the ubiquity of the Internet and the fact that sites hosted outside the United States appear as seamlessly as those hosted within the United States. Therefore, new legal tools are necessary to further counter the threat of jihadist websites.

An aggressive application of current statutes may suffice to counter these websites by targeting material supporters. Treasury's designation process, if liberally and aggressively applied, may also provide an adequate remedy. As detailed earlier, subparagraph three of Executive Order 13224 allows Treasury to block both property and interests in property that "act for or on behalf of" those parties already designated as terrorist organizations. Furthermore, subparagraph four allows similar techniques to be applied to "individuals or entities that 'assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of 'such acts of terrorism or those parties already designated.'"[59] A broad interpretation of these rules would result in the blocking of both property and interests in property for jihadist website supporters.

Nevertheless, this process is limited because these entities may not have assets worth blocking. Thus, a true cyber embargo would entail creating a new process whereby those foreign

[54] *Id.* at 377.

[55] *See* Teague v. Reg'l Comm'r of Customs, Region II, 404 F.2d 441, 445 (2d Cir. 1968).

[56] Global Relief Foundation, Inc. v. O'Neill, 207 F. Supp. 2d 779, 806 (N.D. Ill. 2002), citing Humanitarian Law Project v. Reno, 205 F.3d 1130, 1135 (9th Cir. 2000); Palestine Info. Office, 853 F.2d at 939-40; *cf.* Walsh v. Brady, 927 F.2d 1229, 1234-1235 (D.C. Cir. 1991)).

[57] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).

[58] Schenck v. United States, 249 U.S. 47 (1919).

[59] Exec. Order No. 13,224.

communications companies that provide material support to terrorist organizations may be designated as "cyber supporters." Such a designation would prevent US companies from conducting business with designated entities. This process would create a virtual *persona non grata*. The interconnected nature of the World Wide Web requires that even those overseas companies that provide Web services to terrorist organizations (the material supporters) must still rely on other Web service providers, many of which are in the United States, to communicate. This reliance is the weak link in the cyber jihadist's Web presence. Designating overseas Web providers as "cyber supporters" forces those companies to choose between either losing all commercial services from the United States or continuing to provide services to the terrorist organization.

How would such a designation work? I propose amending the US Code to create a category of "designated cyber supporter." US companies would be forbidden from engaging in commercial services with entities bearing such a designation. The designation would include elements of the material support statute but would limit itself to Internet companies. Moreover, the designation could include a provision that provides notice and a safe harbor provision that allows companies to sever ties to terrorist organizations to avoid being designated a "cyber supporter."

Diplomatic efforts could further expand the cyber embargo. Initially, this diplomatic effort need not be expansive. Rather, it could focus on the nine countries that control 95.58 percent of all domain registrars.[60] Preventing these registrars from engaging in commercial activity with "material supporters" would have a dramatic impact on the designated entity, likely forcing it out of business if it did not sever its ties to jihadists. Diplomatic efforts have worked in the past, albeit on a small scale. For example, the US Department of Defense reportedly used its leverage to shut down Palestinian resistance sites hosted by the Ukraine in 2004.[61] In another instance "the British government, responding to the U.S. request under the Mutual Legal Assistance Treaty between the two countries, ordered the closure of twenty media websites in seventeen countries that advocated terrorism."[62] Working through diplomatic channels to shut down foreign companies that serve as material supporters is the critical next step in countering the cyber jihad.

As each country cuts off Internet support within their jurisdiction, terrorist Web sites will be forced to find support in new jurisdictions. Continued monitoring and diplomatic efforts would thus remain critical. Additionally, because 95.8 percent of all domain registrars are located in nine countries with which the United States has strong diplomatic ties, the internationalization of these efforts is achievable. Furthermore, internationalizing an agreement that will ensure that other countries shut down "designated cyber supporters" is the next step in countering jihadist websites.

Continuing diplomatic efforts to prohibit dealing with designated cyber supporters will create a system whereby terrorist organizations will have extremely limited choice of locations where they can register and operate their Web sites. In most cases, the Internet jihadists will be forced to register in small, already ostracized countries such as Iran or Libya, which maintain control over their respective .IR and .LY domain names. By limiting internet jihadists to these countries,

[60] Within those nine countries, there are 522 Accredited Domain Name Registrars, 281 of which are located in the United States (54 percent); 124 of which are located in Canada (28 percent); 16 of which are located in Germany (3.07 percent); 12 of which are located in the United Kingdom (2.3 percent); 11 of which are located in the Republic of Korea (2.11 percent); 10 of which are located in Australia (1.9 percent); 8 of which are located in France (1.53 percent); 8 of which are located in Japan (1.53 percent); and 6 of which are located in Spain (1.14 percent).

[61] Al Click, "The Pentagon Closes Jihad Websites," *Guerrilla News Network*, Dec. 29, 2004, available at *http://alpinestar.gnn.tv/headlines/547/The_Pentagon_Closes_Jihad_Websites* (last visited Oct. 19, 2007 (original on file with author).

[62] Rachel Ehrenfeld, "Shutting Down Cyberterror," Oct. 21, 2004, *http://www.frontpagemagazine.com/Articles/Printable.asp?ID=15605*.

diplomatic measures, such as trade restrictions can be brought to bear. Those countries that host jihadist Web sites will then have to decide if they are willing to protect the Internet jihadists at the cost of jeopardizing trade relations.

CONCLUSION AND IMPLICATIONS

Given the ubiquity of the Internet and the challenges of tracking constantly moving Web sites, domain name registrars, and ISPs, one may be left to conclude that efforts to counter the Internet jihad are pointless. Nevertheless, the only truly effective way to counter the Internet jihad is to continually make efforts to shut them down. Doing so can dramatically impact the terrorist Web presence.

The limited efforts of watchdog groups prove that the fight against cyber jihadists is not a fruitless one. Through increased support of watchdog groups, expanded shaming techniques, and the use of existing statutes, terrorist Web sites can be forced to overseas service providers. This first step is not enough, however, as the World Wide Web is dynamic, and the move to overseas service providers will allow cyber jihadists to seamlessly maintain their Web presence. Thus, more aggressive use of existing designation techniques and the creation of a new "cyber supporter" designation are necessary to create a cyber embargo of jihadist Web sites and those companies that provide them services. Diplomatic efforts are necessary to fully realize the potential of the cyber embargo, as cyber jihadists can continually move and find new "cyber supporters" in other jurisdictions. Through continued diplomatic efforts, terrorist Web sites can be forced to exist in a geographically limited number of jurisdictions.

Furthermore, even if only some jihadist sites are closed down, the jihadists will still be restricted to a few overseas hosts. These few hosts would no longer be needles in a haystack---instead with fewer places to go, the major jihadist sites with direct links to terrorism could be quickly identified and monitored by investigators---effectively corralled into places where they could be more closely monitored.[63] The end result of this process will not eliminate the cyber jihadist presence, but geographically limiting terrorists allows for government and civilian orchestrated monitoring, as well as for offensive actions to shut down these sites.

Some Web sites might, for intelligence reasons, be identified as sites that the government will not want to shut down. Instead, the government may choose to monitor or compromise these sites as they may contain valuable intelligence information, such as user names, locations, and messages that users believe to be encrypted but are in fact being monitored. While some advocate for this technique, it is important to note that it is not universally accepted, as some contend "getting real actionable intelligence from a terrorist website or forum is extremely difficult and requires a lot of time and a lot of luck[,] and in many cases the small amounts of available actionable intelligence would only be noticed after the act is done."[64] Thus, geographically limiting these sites will corral the cyber jihadists onto a limited number of web servers, effectuating monitoring and other counterterrorism techniques.

While some may argue that the anonymity of the Internet makes locating and shutting down jihadist Web sites too challenging, one must bear in mind that jihadists use Web sites for the specific purpose of dispersing information and connecting with each other. To a large extent, jihadists are

[63] *See id.*

[64] Jerry Gordon, "Fighting Internet Jihad: An Interview with Joseph Shahda," *New English Review* (2007), *http://www.newenglishreview.org/custpage.cfm/frm/11995/sec_id/11995.*

forced to relinquish anonymity in order to reach their own audience.[65] In addition, anonymity is a two-way street. Trackers and investigators can infiltrate the jihadist ranks by acting as interested jihadists, avoiding detection through anonymity.[66]

The key to countering jihadist websites is to relentlessly target them, keeping them continually on the move, cutting off their resources by targeting "cyber supporters," and, finally, limiting their potential areas of operation so that increased monitoring and other counterterrorism techniques can be applied to them. Following these steps will go a long way toward addressing the technical and political issues inherent in the Internet jihad that have plagued lawmakers and policy experts.

[65] *See* A. Aaron Weisburd. "Global Jihad, the Internet and Opportunities or Counter-terrorism Operation," *Internet Haganah*, Aug. 23, 2005. *http://internet-haganah.com/harchives/004824.html.*
[66] *See id.*

Mr. SHERMAN. I thank you, Professor, and since you are suggesting legislation—my law school professors used to assign homework. I have always wanted to reverse that. So if you haven't done so already, your homework assignment is to draft proposed legislation implementing what you are talking about. Unless you have already done that.

Mr. MCNEAL. Mr. Sherman, I would be happy to work with the committee on drafting that legislation.

Mr. SHERMAN. And they say this job doesn't have perks. I just gave a homework assignment to a law professor.

We are going to hear, first, questions from our ranking member, Mr. Royce.

Mr. ROYCE. Let me ask a question of Mansour. You mentioned that your move away from radical Islam or jihadist thinking came as a result of an article that you read. I wondered if you had read that on a Web site or if it was a pamphlet. I am wondering how that idea got in circulation. You were in Sudan, I think, at the time?

Mr. AL-HADJ. Saudi Arabia.

Mr. ROYCE. Saudi Arabia. I would also ask if—that is Khales—what did you say his name was? Khales Jalabi?

Mr. AL-HADJ. Khales Jalabi, yes.

Mr. ROYCE. Is he widely read today? Is there sort of a movement in Saudi Arabia?

No, not really?

Mr. AL-HADJ. Not really. He basically is considered like a bad guy or something because he is against jihad. I mean, he interprets Koran and jihad in Koran in another way, in a peaceful way, and the radicals don't like him.

Mr. ROYCE. Tell me a little bit, real quickly.

Somebody behind you wanted to make a comment, I guess.

Ms. ALHANI. Yes, because you were asking him about Khales Jalabi, I would just add something he didn't know maybe, that he is a Syrian writer. He writes—but, as you know, a writer. He is Islamic, but he is not a radicalist or criminalist either.

Mr. ROYCE. I see.

Mr. SHERMAN. Normally, we don't hear from anyone sitting in the audience, but you are allowed to—but the one requirement is that the woman who just spoke needs to identify herself for the record. Can you give us your name, please?

Ms. ALHANI. I am Fawziah Alhani. I am a human rights activist. I was attending another conference here.

Mr. SHERMAN. Thank you for your name.

Mr. ROYCE. What I was trying to understand better was, in society, you went to a particular school and in that school these ideas were prevalent. Was the institution that you were in dissimilar in some ways to other schools or do you think this is sort of the mindset that many teachers have?

Mr. AL-HADJ. Yes. I went to college in Sudan, the International University of Africa. In that university there are students from all parts of Africa and the world. Actually, there are American students, too.

That is an Islamic university. The things that they are teaching there are just anti-Western things; and, actually, one—many of the students at the time when I was there, they go and wage jihad. They are highly respected. They don't have to attend any classes, and they would really pass the exams without anything. And, actually, one of my professors died—he lost his life in this jihad.

So the Islamist Government of Sudan, doing this, you know, to spread their ideology, they want to have as many Islamic States in Africa or around the world. So they are spreading this through bringing students, giving them free scholarships to come to this particular school, and teaching them this anti-Western and anti-human rights and things.

So the day of the 9/11, when the Towers hit, I was there. I was a student there, and all that you hear is the cheers and people were very happy, without knowing what happened, who did that. Just because America was hit, it's something very happy for them.

Mr. ROYCE. I have been to Sudan and Darfur. One of the concerns I have about the particular institutions that we are talking about is the way they push martyrdom but also the way they pushed sort of a genocidal campaign, originally in South Sudan, and now it is in Darfur. But in South Sudan that is when you were there, they were pushing this idea.

And just to get off the topic for a minute, is it realistic to think that the government in Khartoum, with this recent history of promoting the type of jihad that we saw carried out, including the genocidal campaigns, would be willing to allow for the south to secede if that is the referendum's outcome that is in Sudan? You don't have to answer that, but I do wonder.

The Sudan Government has made this agreement, but given what the old National Islamic Front Government did in terms of creating this atmosphere, I wonder if it is possible for them to live with the result of the referendum in the south.

Mr. AL-HADJ. Well, right now, they are coming with some ideas. They actually are thinking of delaying the referendum; and, you know, they are really bothered by, you know, American support for the right for southern Sudanese to choose whether they stay united with one Sudan or have their own country. But for them that would be problematic, and I don't think they would allow that to happen.

Mr. ROYCE. One other quick question. In Saudi Arabia, how prevalent do you think the teaching in the textbooks and so forth—what is the prevailing view on this kind of activity? What is the mindset in the schools?

Mr. AL-HADJ. Well, I was—I went to school in Saudi Arabia, and the textbooks are really—they are anti-Western things. They teach us that, you know, a Muslim and Jewish are enemies at the end of the day, and sometimes in the future they will fight each other. And even the trees and stone will help the Muslim kill the Jewish. So these things, I—you know, they taught me these things.

Mr. ROYCE. Yes.

Mr. AL-HADJ. And one of the things that, you know, I now feel really sorry about it, that, in the past, they taught us the story of our Prophet Muhammad killing a whole tribe, the Banu Qurayza tribe in Medina, because of treason or something. When I hear that story, when I was young, you know, it didn't make any difference.

I didn't feel any sorry. I didn't think that the Prophet, you know, had done something really horrible.

So, you know, there is no way of questioning the history of Islam. And, actually, right now, one religious guy in Saudi Arabia, he is one of the writers of the textbooks, the new textbooks. He is really radical, and he actually wants to have like separation in the grand mosques so women can be, you know, on one side and men can be on the other side, and he is one of the people who is writing the books for kids.

So it is in there, and it needs to be reformed.

Mr. ROYCE. If I could ask one more question, and I will ask that of Dr. McNeal.

You mentioned in your testimony, Dr. McNeal, that Treasury has not aggressively attempted to cut off cyber services to terrorism supporters, not even key al-Qaeda facilitators. I was going to ask you why, and what grade would you give that effort in the last administration as well as in this administration? What is afoot here?

Mr. MCNEAL. I would be hesitant to give a, grade only because I haven't seen all the papers before me to grade all of them. But Treasury can do more, and it is obvious they can do more. In my written remarks, I highlighted a Web site of a key al-Qaeda facilitator who is still receiving domain-name services from a company in Oregon. This was as of Monday, I conducted the search and found the Web site myself. It included some Google-translated passages of advocacy of jihad. So that suggests to me on the surface that there could be a resource issue or a focus issue.

So that is not meant to disparage the efforts of those at Treasury, but, rather, suggest that maybe greater direction or focus needs to be placed on this problem. And I don't think across the executive branch there has been a focus on these Web sites, as indicated by both your opening remarks and Congressman Sherman's opening remarks. So it is a matter of motivation rather than a matter of desire, I think.

Mr. ROYCE. Thank you.

I am out of time. I yield back, Mr. Chairman.

Mr. SHERMAN. Thank you, Mr. Royce.

I should point out that Congressman Ellison may be back. He is not a member of this subcommittee, but he does have the great honor of serving on the full committee, and he will be allowed to ask questions of the witnesses after members of the subcommittee have completed their questioning.

With that, I will recognize Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Al-Hadj, your testimony and your comments are both enlightening and yet troubling, because it seems to me the culture of many of our Muslim countries and the whole attitude of the younger generations that are coming along, the anti-West, anti-United States, anti-Jewish sentiment appears to be growing instead of receding. Is that a fair statement?

Mr. AL-HADJ. I think so, yes, because of many things. These things, they are in the saying of the prophet. And the media in the Middle East is always trying to show the U.S. as the cause of every problem on Muslim people around the world. So it is an anti-Western notion that really keeps on growing. And something that the

Muslim community here in the United States are not doing is to speak out and go and tell people that we are not disenfranchised here in America. We enjoy all the freedom and things.

I came to this country 5 years ago. And when I chat with my friends, they ask me, Hey, are you allowed to go to the mosque? Does nobody cause you any problems? Are Muslims hated in America? But this is not true. I don't see an anti-Muslim thing. But when you see the media and the Muslim activists or Muslim organizations when they appear in the media, they are always trying to make themselves as victims, and there is really anti-Muslim things going on in America, but this is not true.

Mr. SCOTT. There has to be some element of responsibility taken by the leadership in some of our more moderate Muslim countries. What is holding that back? Is there a fear, there is a reluctance? Because no matter what we do—I mean, if somebody hates you because you are Jewish or if somebody hates you because you are from the United States, no matter what we do, we are not the instrument that can change that.

Something has to change within the culture over there, and I just don't see positive forward leadership on the part of people who you would feel—educated, who work with this country, have relationships with it—not taking the leadership in these Muslim communities to correct this perception. No matter what we do, we may get interception dealing with the Internet, but that is not going to stop until we can change some attitudes and reverse this trend of anti-Americanism and anti-Israel and Jewish feelings within the Muslim world.

Quite honestly, the tragedy of the situation is that if it does not happen, we are headed down a very, very dangerous road here if we don't get some cooperation from the Muslim world and the leadership to help correct this perception. Because if what you say is true of how these younger people are just getting this hatred, unfounded, we are not the answer to that because we are the devil to them, we are the Satan to them. It has to come from the Muslim community itself.

I don't want to belabor that, but I hope we have some signs of hope there. Do we? Do we have some signs of hope that we can get some counter—to me that is the best counterterrorism we could have, help coming from the Muslim communities to straighten out a lot of the misinformation that is formulating these attitudes that make these young people ripe for recruitment.

I just came from a trip over into Africa and went into the Casablanca area. And that country, Morocco, surprisingly, is a leading country in recruiting terrorists. And supposedly it is our friend. I mean, we give money there, Rick's Cafe is there; a great American movie was named for it called Casablanca—you probably don't remember that—starring Humphrey Bogart some years ago.

But anyway, I would hope that this committee hearing can at least—we can make a dramatic statement that we need to get greater cooperation from the moderate Muslim leadership in the world to help us in this. I think that is going to be the way it will do.

But let me ask you, Mr. McNeal, in your testimony you wrote that independent watchdog sites stand in the best position to monitor jihadi extremist sites. Let me ask you in relationship to that, what is being done to ensure that independent watchdog sites are acting legally and appropriately?

Mr. MCNEAL. It would be difficult to imagine how, short of them shutting a Web site down themselves, how they would be violating the law. Generally, these independent watchdog sites monitor these Web sites and then use shaming techniques to try to get the Web sites shut down.

We heard Mr. Al-Hadj's example about—I think it was 32 out of 50 or something, pretty good result, of Internet service providers who, once they are notified that these jihadist Web sites are present on their servers, they shut them down voluntarily. And so, short of these watchdog groups engaging in some sort of denial of service attack, there isn't a violation of the law there.

And I think actually that these watchdog groups should be encouraged in that respect, because the Web is so expansive, the Web sites are so dynamic in switching servers that the Federal Government wouldn't be able to do it on its own. This is sort of the equivalent of your local neighborhood watch providing tips to law enforcement about crimes being committed in the community.

I think the shortfall is that when these Web sites inform law enforcement—or Treasury, let's say, about the presence—when these watchdogs inform law enforcement about the presence of these Web sites, it is not always followed up on. And we have tools to issue cease-and-desist orders to Web hosts who are providing services to designated groups; however, if it is a nondesignated group, it is just a person advocating jihad, there is currently no law which allows us to have that type of material removed from a Web site. The YouTube examples that were cited earlier are a prime example of that. But I think for the most part these groups, unless they are conducting direct attacks against Web sites, are not violating the law.

Mr. SCOTT. Okay. Let me go back to you for a moment, Mr. Boucek—I don't mean to murder everybody's name up there, but I did get McNeal right. I could handle that.

You wrote that to get ahead of al-Qaeda and Islamic extremism more broadly, we will need to shift to be proactive and not just reactive.

That brings me to the point I mentioned first in my questioning with Mr. Al-Hadj; and that is, what more can we do to encourage the moderate voices? Because I sincerely believe this is the key going forward. We have got to figure out a way to break down this wall and to turn this attitude around or else we are just chasing our tail here.

What do you think more we could do to encourage the moderate voices in the Arab and Muslim world, some that have already, to a degree, spoken out against violence and extremism? What more can we do, or should we be doing to encourage this? Are you satisfied with where we are?

Mr. BOUCEK. Thank you very much.

I think this is an excellent question. I think there is an awful lot that we can do, because there are an increasing number of moderate voices speaking out against violence in the region. I think you could come up with a huge list of clerics and sheiks and officials throughout the Muslim world, in Saudi Arabia and Egypt, who have spoken out saying that violence and terrorism is wrong and have taken action to criminalize these activities.

I think there are things we can do to help get that message out. I think we can begin by probably starting from a position that we need to know more about them so we can talk about them. But also I think there are ways that we can help get those messages out by promoting cooperation amongst different countries. So sharing best practices and technologies for how to get these messages out, how to do education. I also think there are probably ways that you can manipulate search results and do other things, which is far beyond my technical education.

I think another interesting point that I think leads to something you mentioned earlier in your remarks is this issue of this rising anti-American or anti-Western sentiment. I think there are lots of causes for that. And I think it is not just religious motivation, I think it is a whole range of things from social conditions, governments, education, corruption, that feed into this process. So I think we need to step back and say that there is a much larger cause for it.

I think we also need to recognize that as there are many pathways of how people do get into violence or radicalization, people do step back from it. There is a growing body of research to suggest that people do leave militant groups and terrorist organizations. Once we understand this better, we can help facilitate that process, I think.

Mr. SHERMAN. I will now call upon Mr. Ellison for 5 minutes of questioning.

Mr. ELLISON. Well, let me thank Chairman Sherman for this hearing. I think it is very important. Unfortunately, due to multiple demands, I wasn't able to hear all of the testimony, but I appreciate the work that you all have done. I think it is important.

I think that we don't know nearly enough, and the pursuit of how to be more effective in countering violent radicalization is something we all have to devote more time and energy to. But since I didn't get to hear everything, let me just throw out a few ideas I have had and perhaps I can get your reaction.

I think that what needs to happen most of all here is that these Web sites need to have some competition of ideas. And what I mean by that is that if you suppress a Web site—and any Web site that is proposing violent radicalization or how to—I think you just get rid of it and that is the right thing to do. But one that is just offering these extremist ideas, I think it may be more effective to compete with their ideology rather than simply suppress it. And the reason why is that these people who—it seems to me their essential argument is that America is at war with Islam. America is not at war with any religion. America is at peace with all religions.

But if they want to argue that America is at war with Islam, the most effective thing to do is not simply to suppress the argument, but to actually take that argument head-on by talking about a number of things like our Constitution and freedom of religion, by talking about how Muslim Americans are doing, actually prospering pretty well; by talking about how leaders like Michael Bloomberg have stood up and said that the Manhattan Islamic

Center has as much right to be there as any other institution does; how the President stood up and spoke on this issue; and how leaders—Muslim, Christian, Jewish of various faiths—said that the threatened Koran burning was reprehensible.

I mean, I think that we should take on this claim that America is at war with Islam, because I am clear that it is not; and yet if we just suppress it and don't really offer a competing vision, then we may be missing an opportunity, and we might even hand these people an opportunity to say, See, this is just them trying to—they don't want you to hear our side, kind of, argument.

Let me also offer you these ideas because I know the title of this hearing today is Jihadist Web sites. Personally, I don't like the terminology. And the reason why is that, to a Western audience the word "jihad" is a foreign word, it sounds scary, it is certainly used in a scary way, and so it whips us up over here in America. But to the Arabic-speaking world, it is much more akin to the term "freedom fighter." So why would we let——

Mr. SHERMAN. Mr. Ellison, in my opening remarks I did comment on the preferred term being something along the lines of "terrorist" or "extremist," and discussed how the word "jihadist" might——

Mr. ELLISON. Yes. And that is not meant as a critique, and I appreciate your acknowledging that, Chairman Sherman. And let me just say this quite simply, and you all may agree or disagree, from the standpoint of Anwar al-Awlaki, he wants to associate what he is talking about with Islam so that he can go out to the Muslim world and say, I am the standard bearer for Islam and I want you to do this in defense of Islam. Well, we should strip them of that and say, You are not representing Islam, you are representing murder and killing. And so they would love to use Islam as a veneer to sort of market their ideas, and I think we should really figure out how do we deny them that.

I was making this point with somebody a few months ago and they said, Well, this is what they call themselves. I said, Well, that is exactly why we shouldn't call them that. None of us would say that Timothy McVeigh is a freedom fighter, even if he called himself that; we call him a mass murderer. Well, we should call Anwar al-Awlaki a promoter of mass murder and we should call Osama bin Ladenan actual mass murderer.

So whenever we say Islamic terrorists, Islamic—we are always associating it with Islam. I think that we think we are standing up against the bad guys, but I think we may unwittingly be actually helping to reinforce their argument.

I haven't dropped it yet, but I am actually really sort of thinking a lot about perhaps a study bill on violent radicalization. I know Jane Harman has done this in the past. It was met by many people in the civil rights and civil liberties community with opposition, because they thought it would lead to violation of human and civil rights.

I guess I am running out of time, but if I may, could I wrap up, Mr. Chairman?

Mr. SHERMAN. You may.

Mr. ELLISON. I think that we don't know enough about the topic, which is why we profile, which is why we stop the guy with the worry beads and the beard and kick him off the plane, when we are letting the other one go by who is the real danger.

I have pontificated long enough. Thank you very much for listening. And if there is ever any time, I would love to hear your views on what I said.

Mr. SHERMAN. I thank the gentleman.

I would comment that in my district, a mosque is being built, and the only controversy is whether it has enough parking spaces.

An article in the Case Western Reserve University Journal of International Law discusses the strategy for containing and removing terrorist material through a process of shaming those who provide the Web sites to extremists. Limiting the countries which host these Web sites, they argue, will make it easier to track and control.

Dr. Boucek, is the strategy of just naming, shaming, viable? And in particular, in your testimony you talk about YouTube, and apparently al-Qaeda in the Arabian Peninsula has a site. I know I have a site, Keith has a site, David has a site. Is that site still up just because nobody has bothered to contact YouTube, or is it up because YouTube has decided to leave it up?

Mr. BOUCEK. Thank you very much.

Taking your last point first, I cannot tell you why it is still up. At least earlier this week, on Monday——

Mr. SHERMAN. Are you aware of anybody who has contacted YouTube and said, "Hey, do you know about this?"

Mr. BOUCEK. There are some people who have mentioned this before. I don't think it is very well known that there is this site. Probably more disturbing, the video content that is available has been replicated across any number of other sites now. The very concerning thing to me, though——

Mr. SHERMAN. You obviously find these sites. When you personally find them, do you drop a line to YouTube? Do they read their mail?

Mr. BOUCEK. In this case, no, I have not.

Mr. SHERMAN. Well, homework assignments are not limited to law professors. To start this out, give me a list of the sites. I will put a letterhead on top of it just to make sure that it is read by somebody at a more senior level and we will see what happens.

Mr. MCNEAL. Chairman Sherman, just on that point, may I interject?

Mr. SHERMAN. Yes.

Mr. MCNEAL. About a year ago, Senator Lieberman sent letters to YouTube requesting this, and their response was they will evaluate content that is flagged as inappropriate, but they value individuals' free-speech rights. So we have a legal limitation because under section 230 of the Communications Decency Act, Web providers, it is up to them whether or not they can take something down and determine whether or not it is obscene.

Mr. SHERMAN. Well, this is not obscene; this is put up by a terrorist organization. This seems to have some of the content of al-Qaeda in the Arabian Peninsula. This is the official site of al-Qaeda. I don't think there is any doubt that our terrorism laws do not allow U.S. corporations to do business with terrorist organizations.

Mr. BOUCEK. I am able to explain why this particular YouTube channel is still available.

Over the summer, in July——

Mr. SHERMAN. Well, we have a law professor here as well. Let's say somebody is inspired by this site, and let's say they kill somebody; are you certain that YouTube would escape civil liability?

Mr. MCNEAL. I am certain they would escape criminal liability. I am not certain if they would escape civil liability. I believe the issue and the argument that was put forth by YouTube, when this came up last year, is that it is difficult for them to isolate the identity of who it is. And so their site may say, We are the official YouTube channel of al-Qaeda in the Arabian Peninsula. But YouTube is unable to verify that, and therefore their policy is one of openness and dialogue and shout-down, that type of thing.

Mr. SHERMAN. Terrorism laws would be absolutely meaningless if you could do business with a terrorist organization operating under its own name and say, "Well, there was no certified letter from a deity proving that there was in fact a terrorist organization."

Mr. MCNEAL. Chairman Sherman, we are in agreement on this. I think that more action needs to be taken and screws need to be turned against these service providers, whether they are the biggest, YouTube, or the smallest——

Mr. SHERMAN. Well, I don't know how much money YouTube makes and how much its executives make, but they are endangering people throughout America for their own profit. And it is not out of great loyalty to the concept of the First Amendment, it is out of great loyalty to money. They feel that if they let everybody on, that just makes a little bit more money for them. And for them to endanger lives nationwide for that reason is a decision that they have made. And if they want to take down my site, they are welcome to. As a matter of fact, this will be up on my site.

Yes.

Mr. BOUCEK. I think the only point that I can contribute to this is that in the beginning of July there was the release of this English-speaking magazine, "Inspire," that you had alluded to in your opening remarks. Shortly thereafter, this channel appeared. I think one can draw the conclusion that there is a connection. As of this week when I checked this channel, all of the videos are still available, and this person is accessing this site frequently and updating this material.

Mr. SHERMAN. So this is a secondary site that is taking its content from the site of YouTube——

Mr. BOUCEK. No. This is the YouTube channel that we have been discussing.

Mr. SHERMAN. Okay. So this is a channel that brands itself as the official site of al-Qaeda in the Arabian Peninsula.

Mr. BOUCEK. That is correct. It brands itself as the media arm for AQAP. And the very concerning thing, which I think we have all highlighted, is that you no longer need to have much knowledge or language capacity to access this. You can get all of these videos and you can consume them, just knowing English from anywhere.

Mr. SHERMAN. Now, does the content of this site advocate violent action against Americans?

Mr. BOUCEK. I think al-Qaeda in the Arabian Peninsula has been very clear about its positions.

Mr. SHERMAN. I know what their positions are, but in terms of what they have chosen to put up.

Mr. BOUCEK. In some of the videos they have been advocating violence against American interests, American allies, American partners. I think that there is no reason why this should be available. I can't give you an answer on that.

Mr. SHERMAN. And is there material there that provides useful information to those who wish to be terrorists as to how to make a bomb, how to sneak in a bomb?

Mr. BOUCEK. Just real quickly I would say, as opposed to "Inspire" magazine that provides actual tactical information—how to assemble explosives, what to bring on jihad, how to engage in operations—what this does is provide you with the theological and ideological justifications to get you to that point.

Mr. SHERMAN. Okay. But it is a little bit more provable that something is reprehensible when it says, Here is how to make a bomb, rather than, "Here is why American foreign policy is so bad that you should hate America." There are aspects of U.S. policy that I personally hate.

Let me hear from Mr. Al-Hadj.

Mr. AL-HADJ. Thank you, Mr. Chairman.

As I was coming to this hearing, one of the jihadi Web sites linked its site to a Facebook account. And the last thing I saw was a post on how you can make a car bomb like the one Faisal Shahzad did. And they are encouraging people, like specific details on how you can make——

Mr. SHERMAN. I am going to ask you to suspend for just 1 second.

Please proceed.

Mr. AL-HADJ. Yes. As I was coming here, there was this post on Facebook——

Mr. SHERMAN. And let me just remark for the record, the U.S. Government does have efforts to put things up on the Web that are part of our public diplomacy program to debunk what terrorists have to say. I know that is important to the gentleman from Minnesota.

As to whether there will be further efforts is something I can talk to him about on the floor. But I do think the record should reflect that while we are discussing what the terrorists are doing on the Web site, we are of course using the Internet to communicate a much more wholesome message.

The gentleman will proceed.

Mr. AL-HADJ. So Facebook was posting the same post that was on this jihadi Web site, encouraging lone wolves or individuals who want to persecute an operation or a suicide mission, how specifically—with small details how to make a car bomb, what should you buy, like materials, easy materials, very accessible to everybody—how you can make a car bomb and do it.

Mr. SHERMAN. So you go to Facebook, and then that refers you to a site that gives you not just ideology, but "how to" practical information for terrorism.

Mr. AL-HADJ. You go to the jihadi Web site and there is a Facebook sign on it saying, "You can join us on Facebook." So once you click there, you will receive whatever they post in there.

Mr. SHERMAN. Thank you.

Mr. McNeal, we can always ask somebody to take material down. Some sites in certain countries won't do that. How easy is it for us as a technical matter to just use cyber attack and take the site down?

Mr. MCNEAL. We have the capacity. There was an example I think that you alluded to in your opening remarks that was reported in the Washington Post about a site that was known as—the term in the field is a "honey pot." It is purposefully set up to bring in terrorists and track them. This was a joint operation between the CIA and the Saudi Government.

Mr. SHERMAN. And that is the one we took down?

Mr. MCNEAL. That is the one we took down. But actually, the debate over it was a healthy one that we should be having more of. The reason we took it down is that our commanding general in Iraq, General Odienero, said that this site was in fact costing American lives. And there was an interagency fight between DOD and the Intelligence Community on whether or not to take the site down.

Mr. SHERMAN. Was it taken down because it was a site sponsored by the U.S. Government and they just flipped the off switch, or did we cyber attack a site that another government agency was paying to put up?

Mr. MCNEAL. From the public reports, we took out a site that was run by the Saudi Government, with the cooperation of the Central Intelligence Agency. The rationale for it was that the site was providing information about how to conduct coordinated attacks on U.S. troops in Iraq. And what happens in these types of interagency——

Mr. SHERMAN. Did we use a cyber attack to take it down?

Mr. MCNEAL. Yes, it was a denial-of-service attack. The collateral consequences of that, though, were that not only was this site taken down, there were some sites in Texas and other places that were affected by taking out the server.

The reason these debates come up is—it was partly alluded to in my written remarks, in that there are many who believe that keeping these sites up provides an intelligence value. And so the fight between DOD and the Intelligence Community was that if you leave it up, we could continue to observe and learn more about what these individuals are doing. And that is the primary push from the Intelligence Community's perspective is always to gather more information to connect the dots.

It was healthy, I think, that we had that debate between taking it out and leaving it up, but it was an ad hoc one through a task force, rather than an agency or a division within an agency structure to force us to have that type of communication.

Mr. SHERMAN. Now, with regard to sites that are not maintained by ourselves or other governments that we are cooperating with, are we able to determine at least the e-mail address of those who are visiting the sites?

Mr. MCNEAL. Not necessarily the e-mail address, but IP address logs, server logs, can tell us——

Mr. SHERMAN. That is only if the Web site server and provider cooperates with us. So if there is, for example, in Iran a Web site server and the Iranian Government chooses not to cooperate with us, then by monitoring the site we can know what the terrorists want to say, but we have no idea who they are saying it to.

Mr. MCNEAL. For the most part, that is correct, Mr. Chairman. There are people who, through covert methods, can infiltrate networks and find information out irrespective of the location of the network.

The bigger challenge, I think, is that, particularly with regard to foreign Web hosts, is that because they are beyond the reach oftentimes of U.S. laws, we don't have a lot of ways to turn the screws to them, unless we were to back out sort of one level from that site and, almost like a trade embargo, say that you, Web provider, can no longer do Internet business with U.S. service providers if you continue to provide service to that Web site.

And then the Iranian company, to use your example, would have to choose between supporting this one Web site or losing all of its commercial traffic from the United States. I think that would probably be an easy choice.

Mr. SHERMAN. But the argument is gathering intelligence versus taking down the terrorist site. And the question is, are we really able to gather valuable intelligence? And there are two aspects of this intelligence: What do terrorists want to say? Second, which individuals seem interested in what terrorists have to say—which, by the way, includes many people in this room.

And you are saying that the second type of information is probably available only with the cooperation of the site Web provider.

Mr. MCNEAL. These are more forums than Web sites, so unless an individual posing as a member of the forum could get inside and be seen as a legitimate person who is communicating and supporting ongoing activities.

Mr. SHERMAN. And even if you knew somebody was part of that forum, they might not use their real name.

Mr. MCNEAL. Right. But the goal, Mr. Chairman, would be to engage that person in conversation about operational plots they might want to take part in, and then go from the cyber world to the real world. There are some examples of us doing this in cooperation with law enforcement in Europe.

Mr. SHERMAN. Well, I think we end this hearing with more specific knowledge, but we end this hearing in the same position; and that is that we will use the Internet for our own public diplomacy effort. We will certainly monitor what terrorists have to say, and that will help us with our own public diplomacy. And we will occasionally be able to detect who on these sites mean us harm.

But we are unsuccessful in taking down sites—often we are unsuccessful—by sending people letters, and we are manifestly unable to take down these sites through cyber attack, because we are constrained by our own politeness. And being polite is good as long as it doesn't cost American lives.

So I thank everyone for coming. Additional statements can be made for the record. I believe we are being called for a vote. I want to thank our vice chair and our ranking member for being here at the hearing.

Thank you.

[Whereupon, at 3:05 p.m., the subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

SUBCOMMITTEE HEARING NOTICE
COMMITTEE ON FOREIGN AFFAIRS

U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C. 20515-0128

SUBCOMMITTEE ON TERRORISM, NONPROLIFERATION AND TRADE

Brad Sherman (D-CA), Chairman

September 28, 2010

TO: MEMBERS OF THE COMMITTEE ON FOREIGN AFFAIRS

You are respectfully requested to attend an OPEN hearing of the Subcommittee on Terrorism, Nonproliferation and Trade, to be held in Room 2175 of the Rayburn House Office Building: **(and available live, via the Committee website at http://www.hcfa.house.gov)**:

DATE:	Wednesday, September 29, 2010
TIME:	1:30 p.m.
SUBJECT:	U.S. Strategy for Countering Jihadist Websites
WITNESSES:	Christopher Boucek, Ph.D. Associate, Middle East Program Carnegie Endowment for International Peace
	Mr. Mansour Al-Hadj Director, Reform in the Arab and Muslim World Project The Middle East Media Research Institute
	Gregory S. McNeal, J.D. Associate Professor of Law Pepperdine University

By Direction of the Chairman

The Committee on Foreign Affairs seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202/225-5021 at least four business days in advance of the event, whenever practicable. Questions with regard to special accommodations in general (including availability of Committee materials in alternative formats and assistive listening devices) may be directed to the Committee.

COMMITTEE ON FOREIGN AFFAIRS

MINUTES OF SUBCOMMITTEE ON *Terrorism, Nonproliferation, & Trade* MEETING

Day 9/29/2010 Date *9/29/2010* Room *2175 RHOB*

Starting Time *1:30pm* Ending Time *3:00pm*

Recesses (_____ to _____)

Presiding Member(s) *Subcommittee Chairman Brad Sherman*

CHECK ALL OF THE FOLLOWING THAT APPLY:

Open Session ☑
Executive (closed) Session □
Televised ☑

Electronically Recorded (taped) ☑
Stenographic Record □

TITLE OF HEARING or BILLS FOR MARKUP: *(Include bill number(s) and title(s) of legislation.)*
"U.S. Strategy for Countering Jihadist Websites"

SUBCOMMITTEE MEMBERS PRESENT:
Brad Sherman, Ed Royce, David Scott, Donald Manzullo

NON-SUBCOMMITTEE MEMBERS PRESENT: *(Mark with an * if they are not Members of HFAC.)*
Keith Ellison

HEARING WITNESSES: Same as meeting notice attached? Yes ☑ No □
(If "no", please list below and include title, agency, department, or organization.)

STATEMENTS FOR THE RECORD: *(List any statements submitted for the record.)*

ACTIONS TAKEN DURING THE MARKUP: *(Attach copies of legislation and amendments.)*

RECORDED VOTES TAKEN (FOR MARKUP): *(Attach final vote tally sheet listing each member.)*

Subject	Yeas	Nays	Present	Not Voting

TIME SCHEDULED TO RECONVENE ______
or
TIME ADJOURNED ______

____
Subcommittee Staff Director