USING THE WEB AS A WEAPON: THE INTERNET AS A TOOL FOR VIOLENT RADICALIZATION AND HOMEGROWN TERRORISM

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

NOVEMBER 6, 2007

Serial No. 110–83

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
48–978 PDF WASHINGTON : 2009

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 HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

JANE HARMAN, California, *Chair*

NORMAN D. DICKS, Washington
JAMES R. LANGEVIN, Rhode Island
CHRISTOPHER P. CARNEY, Pennsylvania
ED PERLMUTTER, Colorado
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DAVID G. REICHERT, Washington
CHRISTOPHER SHAYS, Connecticut
CHARLES W. DENT, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

THOMAS M. FINAN, *Director and Counsel*
BRANDON DECLET, *Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
DERON MCELROY, *Minority Senior Professional Staff Member*

CONTENTS

USING THE WEB AS A WEAPON: THE INTERNET AS A TOOL FOR VIOLENT RADICALIZATION AND HOMEGROWN TERRORISM

Tuesday, November 6, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING,
AND TERRORISM RISK ASSESSMENT,
Washington, DC.

The subcommittee met, pursuant to call, at 2:00 p.m., in Room 311, Cannon House Office Building, Hon. Jane Harman [chairwoman of the subcommittee] presiding.

Present: Representatives Harman, Dicks, Carney, Langevin, Reichert and Dent.

Ms. HARMAN. Good afternoon. Our hearing, Using the Web As a Weapon: The Internet as a Tool For Violent Radicalization and Homegrown Terrorism, will come to order.

Last month, the New York Times introduced the world to Samir Khan, a 21-year-old American living at his parents' house in North Carolina. Khan has been operating one of the most active English language Web sites on the planet, one that promotes a radicalized view of Islam and violence against Americans here at home. It hosts hundreds of links to videos showing American soldiers being killed by Iraqi insurgents, including a file called, "The United States of Losers," which showcases a recent news broadcast about a fire fight in Afghanistan.

Kahn's commentary on the site reads, "You can even see an American soldier hiding during the ambush like a baby. AllahuAkbar! AllahuAkbar!"

Kahn's is not an isolated case. This past August, Ahmed Mohammed and Youssef Megahed, 21-year-old University of South Florida engineering students, were stopped for speeding in Goose Creek, South Carolina. The stop resulted in a two count Federal indictment on terrorism related charges. When questioned by Federal agents, Mohammed admitted to using the Internet to post a 12-minute YouTube video demonstrating in Arabic how to turn a toy boat into a bomb. He told the FBI that he made the video to teach, "those persons in Arabic countries to defend themselves against the infidels invading their country."

And in March of this year, Hassan Abujihaad, AKA Paul Hall, was arrested in Phoenix, Arizona, on charges that he supported terrorism by disclosing secret information about the location of

Navy ships and the best ways to attack them. The investigation of Abujihaad, a former U.S. Navy sailor, began with an Internet service provider in Connecticut. Abujihaad is believed to have exchanged e-mails and information with a British computer specialist arrested in Great Britain in 2004 for running terror financing Web sites.

In September of last year, Adam Gadahn, the son of Jewish parents from Southern California who himself converted to Islam and went on to become Osama bin Laden's spokesman, released a 45 minute video on the Internet called, "An Invitation to Islam." In that video, Gadahn talks about al-Qa'ida's ideology, rationale and motivations, encouraging Americans to sympathize with the group.

There can be no doubt, the Internet is increasingly being used as a tool to teach and radicalize Americans and legal residents. These people no longer need to travel to foreign countries or isolated backwoods compounds to become indoctrinated by extremists and learn how to kill neighbors in our communities.

On the contrary, the Internet allows them to share violent goals and plot from the comfort of their living rooms, a problem that the President's own recently released National Strategy for Homeland Security tells us is here and is not going away.

How we address violent radicalization while respecting the Constitution in the process is not easy. There is no magic pill or rule book or law that will fix this. But there are steps to take. Representative Reichert and I are co-authors of H.R. 1955, the Violent Radicalization and Homegrown Terrorism Prevention Act of 2007, which passed the House 404–6, a near miracle, several weeks ago.

The centerpiece of H.R. 1955 is the creation of a national commission to study violent radicalization, to determine the best way forward and to make concrete proposals for action. At 6-month intervals over 18 months, this commission would drill down on the issue and propose to both Congress and the Secretary of Homeland Security initiatives to intercede before radicalized individuals turn violent.

We are not afraid of where the facts will take us, but no one on the Hill or elsewhere should think we already have a complete understanding of how someone with radical beliefs, beliefs which are protected by our Constitution, becomes a violent killer, actions which are not protected and, in fact, which are condemned by our laws and which are felonies.

Many in the Senate likewise support our call for a national commission. My colleague and friend, Susan Collins of Maine, recently introduced companion legislation that would make the commission a reality. I look forward to working with the Senate to get a bill to the President's desk before the end of this session.

I welcome our witnesses today who will tell us about the Internet and how it is a tool of violent radicalization and how it is abused—I would say abused—by those who would call others to commit violent acts. I believe our witnesses' remarks will be a valuable starting point for the national commission's work. I appreciate the fact that you have come here today and now would yield 5 minutes to the ranking member for any opening remarks he wishes to make.

Mr. REICHERT. Thank you, Madam Chair. And I also thank you for holding this hearing.

VerDate Nov 24 2008 13:10 Nov 05, 2009 Jkt 000000 PO 00000 Frm 00006 Fmt 6633 Sfmt 6633 H:\DOCS\110-HRGS\110-83\48978.TXT HSEC PsN: DIANE

As I was listening to your opening statement, I, too, have an opening statement. But I am a storyteller, and I would like to just think about, part of our statement here today is how much the world has changed with the Internet giving us global access and communications, really, for that matter. And one of the stories that I like to share even just going not too far back in history, into the late 1990s, when I was the sheriff and we had a problem with WTO in Seattle. And part of my response to that was to be on the streets with the troops downtown during that disturbance.

Shortly thereafter, a Tacoma police officer took a trip to India. And while he was in the high mountains of India retracing his family roots, he came across a village where his family began years and years and years before. And as he was speaking with these high mountain people in this small community, he told them that he was from Seattle, Washington, the United States of America, in Seattle. And they got very excited and wide-eyed. And he also told them that he was a police officer from Tacoma, and they really got excited. "Do you work for the great sheriff of Seattle?" And he was very surprised and said, "How in the world would you know about the sheriff in Seattle?"

Well, during WTO, I ran down the street and I chased a crook that was ripping off a Radio Shack store in Seattle. And they happened to have one TV and one satellite dish, and so the village was surrounded around this TV watching WTO in Seattle and the one sheriff running down the street chasing after a crook. So after that little story and after he told a little white lie and said that he did work for the great sheriff of Seattle, the red carpet was rolled out for him.

But what an example of how small this world has become. And when you talk about the way that we communicate now and how fast information moves, and now we are moving not only from satellite TV into a small village in India, but we are talking about the Internet and how you can begin to change minds.

The Internet is good in some respects. But, unfortunately, the Internet also facilitates terrorist communications, provides an additional venue for terrorists to spread their hateful and murderous propaganda. The Internet communications established by these terrorists and would-be terrorists serves as a virtual society where otherwise alienated and isolated individuals can meet for training, reinforcement and social networking. Powerful, commercially available encryption and communication tools make these societies hard to penetrate.

A recent report from George Washington University and the University of Virginia found that Internet has made a range of terrorist operational activities cheaper, faster, and more secure, including communications, propaganda, radicalization and recruitment. The New York City Police Department found that the Internet is the driver and enabler for the process of radicalization. Similarly, the United States Institute of Peace noted that, "The great virtues of the Internet, ease of access, lack of regulation, vast potential audiences and fast flow of information, among others, have been turned to the advantage of groups committed to terrorizing our communities to achieve their goals."

VerDate Nov 24 2008 13:10 Nov 05, 2009 Jkt 000000 PO 00000 Frm 00007 Fmt 6633 Sfmt 6633 H:\DOCS\110-HRGS\110-83\48978.TXT HSEC PsN: DIANE

The problem of the Internet radicalization is fairly well documented by these and other studies. But the question remains: What can be done about it? What can we do now? How can we protect ourselves without harming the rights of law-abiding citizens and without doing damage to the free flow of information on the Internet that is now vital to our economy and this information age?

This subcommittee has produced legislation by myself and Chairwoman Harman, which she mentioned, establishing a commission on radicalization to help establish a national strategy to combat terrorism. While this certainly is a good first step, there may be additional interim steps that we can take in the meantime. According to the Middle East Media Research Institute, most Radical Islamist Web sites are hosted on servers based in the West, taking advantage of the very same freedoms they wish to destroy.

It is also true, however, that many of the Western Internet service providers hosting these sites may be unaware that they are facilitating terrorism. So it seems to me that maybe a first step to any Internet counter-radicalization strategy would be to ask responsible Internet service providers to police themselves and voluntarily shut down sites that sponsor terrorist propaganda.

We hope to hear from our witnesses today about their ideas and how we can counter Internet radicalization, reduce its spread and begin to win the war of ideas against those who seek to destroy our culture and our freedoms.

Ms. HARMAN. I thank the ranking member, and now welcome the chairman of the full committee, Mr. Thompson of Mississippi, and yield to him for an opening statement.

Chairman THOMPSON. Thank you very much, Madam Chairman. And I compliment you for having this hearing. As you know, based on the work we have done in the last couple of weeks, it appears that we will do more in this area.

Today we turn to a very serious concern, the use of the Internet to promote extremist violence. The Internet has drastically increased the ability of terrorists to reach a global audience, an audience they want to indoctrinate. And the terrorists are doing so with impunity.

Unlike other pathways into the country, the Internet is not restricted by border enforcement or protected by TSA, and its users can remain anonymous. It allows users to connect with like-minded individuals, resulting in a sense of closeness and community that transcends race, gender, age and physical location. Indeed, the Internet provides users with a sense of belonging, a perfect vehicle for al-Qa'ida and others to recruit people on the fringes, and it is happening.

Daniel Sonier, a 22-year-old troubled Canadian, stated, "The first time I saw an al-Qa'ida video on the Internet, I was ready to go. I wanted to kill the disbelievers." According to one friend, Sonier became so extreme, he once said he would go to war against his own father. Friends started calling him Osama bin Daniel.

What is so troubling about Mr. Sonier is that, by all accounts, he was an average 22-year-old until he was indoctrinated by extremists that found him on the Internet.

Mr. Sonier lives in Canada, but Samir Khan, a 21-year-old old American, operates an extremist Web site out of the comfort of his

VerDate Nov 24 2008 13:10 Nov 05, 2009 Jkt 000000 PO 00000 Frm 00008 Fmt 6633 Sfmt 6633 H:\DOCS\110-HRGS\110-83\48978.TXT HSEC PsN: DIANE

parents' home in North Carolina. It is one of the most frequently visited English language Web sites in the world that preaches a radicalized view of Islam and promotes violence.

What makes the means of communication so appealing to terrorist organizations is that new converts don't need a plane ticket to arrange a meeting. Instead, videos, blogs, chat rooms and message boards expose new recruits to a romanticized view of Jihad with a few keyboard strokes.

I want to congratulate the Chair and ranking member of this subcommittee for authorizing the bill that overwhelmingly passed the House last month. It forces us to take this threat and come up with strategies to counter it that not only protect our people but also their constitutional rights.

I look forward to this hearing today and its testimony. I expect it will be a useful starting point for us to develop strategies to thwart homegrown terrorism. Welcome.

Ms. HARMAN. Thank you, Mr. Chairman. Other members of the subcommittee are reminded that, under committee rules, opening statements may be submitted for the record.

I welcome our panel of witnesses. Our first witness, doctor Bruce Hoffman, is well known to me and has advised me over the years on various issues involving terrorism. In fact, he has been studying terrorism himself for 30 years.

That should have been enough time to solve this problem, Bruce.

He is currently a tenured professor in the securities studies program at Georgetown University's Edmund A. Walsh School of Foreign Service. He previously held the corporate chair in counterterrorism and counterinsurgency at the RAND Corporation, which is where I met him, and was also director of RAND's Washington, D.C., office. He holds degrees in government, history and international relations, and received his doctorate from Oxford. Dr. Hoffman is the author of the book, "Inside Terrorism."

Our second witness, Rita Katz, is the director of the Search for International Terrorist Entities Institute, or SITE, for short. She has studied, tracked, and analyzed international terrorists and their financial operations for many years. Since well before September 11th, she has personally briefed government officials, including former terrorism czar Richard Clarke and his staff in the White House, as well as investigators with the Department of Justice, Department of Treasury, and Department of Homeland Security on the financing and recruitment of networks of the terrorist movement. She is the author of Terrorist Hunter—I am outing her, because the author of this book is called Anonymous—"Terrorist Hunter: The Extraordinary Story of a Woman Who Went Undercover to Infiltrate the Radical Islamic Groups Operating in America." And following her testimony, in fact following the testimony of all of our witnesses, we will show a short video that she has assembled that includes some of the information that is on these sites. I thought that would be useful for our members and also for the audience that is physically here or watching on television. And, let me say, parental discretion is advised.

Our third witness, Parry Aftab, is an Internet attorney and was one of the first lawyers to practice Internet law shortly after the creation of the World Wide Web. Ms.µAftab founded America

Online's Legal Discussions, as well as the Court TV Law Center's Legal Help Line, providing legal information and education to thousands of lawyers, consumers worldwide. Ms.µAftab previously served as head of the U.S. National Action Committee, UNESCO's Internet Safety Project and the World Wide Internet Society's Societal Steering Committee. Her book for parents about online safety has been adapted for worldwide use and has been translated into several languages. She has also worked with law enforcement agencies worldwide in the areas of cyber crime prevention, cyber terrorism, law enforcement and security matters.

Our fourth and final witness, Mark Weitzman, is the Director of the Task Force Against Hate and Terrorism with the Simon Weisenthal Center, and the chief representative of the Center to the United Nations in New York. Mr. Weitzman was also the founding director of the Center's New York Tolerance Center, and is a recognized expert in the fields of extremism and cyber hate. He has lectured and worked with various groups ranging from Congress, the U.N., the EU and U.S. Embassy in Berlin, to the U.S. Army and the FBI. He has also chaired the Working Group on Internet and Media Issues at the Global Forum on Anti-Semiticism that was convened by the Israeli Government in February 2007. The task force coordinates the Center's research and activities on extremism, intergroup relations, the Internet and hate crimes.

Without objection, the witnesses' full statements will be inserted in the record, and I would ask each of you to summarize your statement in 5 minutes or less. There is a clock that I am quite certain is visible to you, and it will start blinking as you near the end of your 5 minutes.

Ms. HARMAN. We will start with Dr. Hoffman.

STATEMENT OF BRUCE HOFFMAN, PROFESSOR, GEORGETOWN UNIVERSITY

Mr. HOFFMAN. Thank you, Madam Chairwoman, and members of the committee, for the opportunity to testify before you on this important issue today.

Terrorism has long been understood to be a violent means of communication. The terrorist act itself is thus deliberately designed to attract attention and then, through the publicity that it generates, to communicate a message. But communication is essential for a terrorist movement, not just to summon publicity and attention but also to promote its longevity and ensure its very survival.

Without an effective communication strategy, a terrorist movement would be unable to assure a continued flow of new recruits into its ranks, motivate and inspire existing members, as well as expand the pool of active supporters and passive sympathizers from which terrorism also draws its sustenance.

Given this constellation of requisite sustainable resources, it is not surprising that terrorists today devote so much time and energy to their communications; that they have fastened on the Internet as an especially efficacious vehicle for this purpose, given its fundamental characteristics of rapidity, ubiquity and cost-effectiveness, is not surprising, either.

Today, virtually every terrorist group in the world has its own Internet Web site and, in many instances, maintains multiple sites

in different languages with different messages tailored to specific audiences. Accordingly, today there are in excess of 5,000 terrorist and insurgent Internet sites worldwide. The ability to communicate in real-time via the Internet has enabled terrorists to reach a potentially vast audience faster, more pervasively, and more effectively than ever before.

The implications of this development have been enormous. The Internet, once seen as an engine of education and enlightenment, has instead become an immensely useful vehicle for terrorists to pedal their baseless propaganda and manifold conspiracy theories, as well as summon their would-be and actual followers to violence.

These sites alarmingly present an increasingly compelling and indeed accepted alternative point of view, a parallel reality that is presented to the terrorists' variegated audiences. Indeed, the Internet's power to radicalize, to motivate, inspire, animate and impel radicals to violence has already been repeatedly demonstrated in the United States, Europe, the Middle East and Asia.

The process of radicalization, abetted, facilitated and encouraged by the Internet, however, is only one side of a coin that critically also involves terrorism subversion. Consider what we have learned about the foiled August 2006 plot to simultaneously bomb ten U.S. airliners and crash them into targets over American cities. This plot, derailed after arrests in Pakistan, once more led U.S. and U.K. officials to yet another terrorist cell of British Muslims of Pakistani heritage. The operation's controller was none other than Abu Ubayadah al-Masri, the commander for al-Qa'ida in Kunar Province, Afghanistan.

Al-Qa'ida may thus be compared to the archetypal shark in the water that must constantly keep moving forward, no matter how slowly or incrementally, or die. In al-Qa'ida's context, this means adapting and adjusting to even our most consequential countermeasures, while simultaneously searching to identify new targets and new vulnerabilities, and continuing to replenish its ranks with new recruits as well as sympathizers and supporters.

In sum, al'Qa'ida's capacity to continue to prosecute this struggle is a direct reflection of both the movement's resiliency and the continued resonance of its ideology and the effectiveness of its communications.

Today, Washington has no such program in the war on terrorism to counter effectively these communications and propaganda. America's counterterrorism strategy continues to assume that America's enemies, be they al-Qa'ida or the insurgents in Iraq, have a traditional center of gravity. It also assumes that these enemies simply need to be killed or imprisoned so that global terrorism or the Iraqi insurgency will both end. Accordingly, the attention of the U.S. military and intelligence community is directed almost uniformly towards hunting down militant leaders or protecting U.S. Forces, not toward understanding the enemy we now face. This is a monumental failing, not only because decapitation strategies have rarely worked in countering mass mobilization of terrorist or insurgent campaigns, but also because al-Qa'ida's ability to continue this struggle is ineluctably predicated on its ability to attract new recruits and replenish its resources. The success of U.S. strategy will therefore ultimately depend on our ability to counter al-Qa'ida's

ideological appeal and thus address the three key elements of al-Qa'ida's strategy: the continued resonance of their message; their continued ability to attract recruits to replenish their ranks; and their stubborn capacity for continual regeneration and renewal.

To do so, we first need to better understand the mindset minutia of the al-Qa'ida movement, the animosity and the arguments that underpin it, and indeed the regions of the world from which its struggle emanated and upon which its hungry gaze still rests. Without knowing our enemy, we cannot successfully penetrate their cells, we cannot knowledgeably sow discord and dissension in their ranks, and thus weaken them from within. We cannot effectively counter their propaganda and messages of hate and their clarion calls to violence. And we cannot fulfill the most basic requirements of an effective counterterrorism strategy, preempting and preventing terrorist operations and deterring their attacks.

Until we recognize the importance of this vital prerequisite, America will remain perennially on the defensive, inherently reactive rather than proactive, deprived of the capacity to recognize, much less anticipate, important changes in our enemy's modus operandi, recruitment and targeting.

[The statement of Mr. Hoffman follows:]

PREPARED STATEMENT OF BRUCE HOFFMAN

Terrorism has long been understood to be a violent means of communication. The terrorist act itself is thus deliberately designed to attract attention and then, through the publicity that it generates, to communicate a message. Indeed, nearly a quarter of a century ago, Alex Schmid and Janny de Graaf observed that, "Without communication there can be no terrorism.[1] But communication is essential for a terrorist movement not just to summon publicity and attention, but also to promote its longevity and ensure its very survival. Without an effective communications strategy, a terrorist movement would be unable to assure a continued flow of new recruits into its ranks, motivate and inspire existing members as well as expand the pool of active supporters and passive sympathizers from which terrorism also draws sustenance.

Given this constellation of requisite sustainable resources—motivated minions, energized recruits, generous supporters and willing sympathizers—it is not surprising that terrorists today devote so much time and energy to communications. That they have fastened on the Internet as an especially efficacious vehicle for this purpose—given its rapid (often in real time), pervasive geographical reach, and cost-effective characteristics—is not surprising either.[2] As Professor Gabriel Weimann of Haifa University notes in his seminal study, Terror on the Internet, when he began studying this phenomenon nearly a decade ago, there were only about 12 terrorist group web sites. By the time he completed his research in 2005, the number had grown to over 4,300—"a proliferation rate," he explains, "of about 4,500 percent per year."[3] And, by the time the book was published the following year, the number had jumped to more than 5,000 terrorist web sites.[4]

Thus, virtually every terrorist group in the world today has its own Internet website and, in many instances, maintain multiple sites in different languages with different messages tailored to specific audiences. The ability to communicate in real time via the Internet, using a variety of compelling electronic media—including dramatic video footage, digital photographs, and audio clips accompanied by visually arresting along with savvy and visually appealing web design—has enabled terrorists

[1] Alex Schmid and Janny de Graaf, *Violence As Communication: Insurgent Terrorism and the Western News Media* (Beverly Hills, CA: Sage, 1982), p. 9.

[2] For a more detailed analysis of historical terrorist communications strategies and their contemporary use of the Internet and other electronic and digital communications means, see Bruce Hoffman, *Inside Terrorism* (NY: Columbia University Press, 2nd edition, 2006), chapters 6 and 7, pp. 173–228.

[3] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace Press, 2006), p. 105.

[4] Remarks by Professor Gabriel Weimann, book launch event held at the U.S. Institute of Peace, Washington, D.C. on 17 April 2006.

to reach a potentially vast audience faster, more pervasively and more effectively than ever before.

The weapons of terrorism today, accordingly, are no longer simply the guns and bombs that they always have been, but now include the mini-cam and videotape, editing suite and attendant production facilities; professionally produced and mass-marketed CD–Roms and DVDs; and, most critically, the lap-top and desk-top computers, CD burners and e-mail accounts, and Internet and worldwide web. Indeed, largely because of the Internet—and the almost unlimited array of communications opportunities that it offers—the art of terrorist communication has now evolved to a point where terrorists can effortlessly and effectively control the communication of their ideology of hate, intolerance and violence: determining the content, context and medium over which their message is projected; and towards precisely the audience (or multiple audiences) they seek to reach.

The changing face of terrorism in the 21st Century is perhaps best exemplified by the items recovered by Saudi security forces in a raid during on an al-Qa'ida safe house in Riyadh in late spring 2004. In addition to the traditional terrorist arsenal of AK–47 assault rifles, explosives, rocket-propelled grenades, hand grenades, and thousands of rounds of ammunition that the authorities the police expected find, they also discovered an array of electronic consumer goods including: video cameras, laptop computers, CD burners, and the requisite high-speed Internet connection. According to "60 Minutes" investigative journalist Henry Schuster, the videos

> had been part of an al-Qa'ida media blitz on the Web that also included two online magazines full of editorials and news digests, along with advice on how to handle a kidnapping or field-strip an AK–47 assault rifle. The videos mixed old appearances by bin Laden with slick graphics and suicide bombers' on-camera last wills and testaments. They premiered on the Internet, one after the other, and were aimed at recruiting Saudi youth.[5]

As Tina Brown, the doyenne of post-modern media, has pointed out: the "conjunction of 21st-century Internet speed and 12th-century fanaticism has turned our world into a tinderbox."[6]

The implications of this development have been enormous. The Internet, once seen as an engine of education and enlightenment, has instead become an immensely useful vehicle for terrorists with which to peddle their baseless propaganda and manifold conspiracy theories and summon their followers to violence.[7] These sites alarmingly present an increasingly compelling and indeed accepted alternative point of view to the terrorists' variegated audiences. This was of course precisely al-Qa'ida's purpose in creating its first website, www.alneda.com, and maintaining a variety of successor sites ever since: to provide an alternative source for news and information that the movement itself could exert total control over. Identical arguments—claiming distortion and censorship by Western and other mainstream media—have also been voiced by sites either created by the Iraqi insurgent groups themselves or entities sympathetic to them.[8] In addition, the Internet has become for terrorists a "virtual" sanctuary to compensate for the loss of their physical sanctuaries and continue to provide information on training and instruction in the means and methods of planning and executing terrorist attacks. Finally, the Internet's power to radicalize—to motivate, inspire, animate, and impel radicals to violence has been repeatedly demonstrated in the United States, Europe and elsewhere.

TERRORISM, RADICALIZATION, AND SUBVERSION

The process of radicalization—abetted, facilitated and encouraged by the Internet—however, is only side of a coin that critically also involves terrorist subversion. Consider what we have learned since the July 2005 bombings of mass transit in London that killed 52 persons and injured more than 700 others. Initially, British authorities believed that the attack was the work of disaffected British Muslims,

---

[5] Henry Shuster, "Studios of Terror: Al-Qa'ida's Media Strategy," CNN International.Com, Tracking Terror, 16 February 2005, accessed at http://207.25.71.245/2005/WORLD/meast/02/15/schuster.column/index.html.

[6] Tina Brown, "Death by Error," Washington Post, 19 May 2005.

[7] See, for instance, the "Iraq" tab at *www.kavkazcenter.com* and the "Iraqi Resistance Report" tab at *www.jihadunspun.com* as well as such sites as *www.islammemo.cc/taqrer/one—news.asp?Idnew=292; www.la7odood.com*; *www.balagh.com/thaqafa/0604ggpz.htm*; and *www.albasrah.net:* all accessed on 6 July 2005. .

[8] "Western Propaganda Media try to shut down albasrah.net! [sic]," the banner on one such site, *www.albasrah.net,* asserted in 2005. "Once again," it argued, "the propaganda media have begun to spew stupid accusations against al-Basrah, the true aim of which is to smother the voice of Iraqi people and smother one of the few sources of information on the unprecedented massacres that are taking place inside occupied Iraq in the name of "international law'." *www.albasrah.net* accessed on 6 July 2005.

self-radicalized and self-selected and operating entirely on their own and within the United Kingdom only. We have subsequently learned, however, that the London cell's ringleader, Mohammed Sidique Khan, and a fellow bomber, Shahzad Tanweer, both visited Pakistani jihadi and al-Qa'ida terrorist camps between November 2004 and February 2005—and, in fact, were trained at al-Qa'ida' Malakand camp in the lawless tribal area along the Pakistan-Afghanistan border.[9]

Both men also recorded "martyrdom" videos while in Pakistan that were subsequently released in September 2005 and then on the first anniversary of the bombings by al-Qa'ida's perennially active communications department, "Al Sahab [the Clouds] for Media Production." On those tapes, Ayman al Zawahiri also claims credit for the London attack in the name of al-Qa'ida: an admission that at the time was mostly dismissed given that it challenged the conventional wisdom that al-Qa'ida was no longer capable of such operations.

In addition, following the bombings, when Khan's photograph was a staple of nightly British newscasts and on the front page of daily newspapers, a reliable source working for Britain's security service claimed to have seen Khan at an al-Qa'ida camp in Afghanistan in either 1999 or 2000.[10] Finally, a BBC documentary broadcast in July 2006 reported that during the summer of 2001 Khan was seen trawling Britain's Muslim communities for recruits to al-Qa'ida—accompanied by two other British Muslims who would later stage a suicide bombing in Israel in April 2003. And, only a month before that attack, Khan himself visited Israel—taking the same route via Jordan that the bombers would soon follow—in what may have been a practice or dry-run for the operation.[11]

The London bombing's pedigree, moreover, is familiar. Exactly a year earlier, British and American authorities had thwarted another plot by a London-based al-Qa'ida cell to simultaneously carry out suicide attacks on the New York Stock Exchange and CitiGroup building in Manhattan, the Prudential Center in Newark, New Jersey, and the International Monetary Fund and the World Bank headquarters in Washington, D.C. The trail in this foiled operation similarly led back to Pakistan. It emerged that a protégé of the 9/11 mastermind, Khalid Sheikh Mohammed, operating in Lahore was the essential nexus between the London cell and al-Qa'ida commanders operating out of Waziristan.

And, a parallel plot disrupted only months before, in April 2004, likewise involved a group of British Muslims of Pakistani ancestry. Their plan was to bomb a shopping mall or—exactly like last June's botched car bomb attack—a London nightclub using 1,300 pounds of ammonium nitrate fertilizer they had stockpiled with which to fabricate their explosives. The leader of the cell, Omar Khyam, had also traveled to Pakistan for terrorist training at the same al-Qa'ida facility in Malakand that two of the July 2005 bombers were trained at. Khyam, admitted that while in Pakistan he had met with al-Qa'ida commanders and that his al-Qa'ida controller for the operation was Abdul Hadi al-Iraqi: the then supposed new "number three" figure in the movement and a key liaison officer with the al-Qa'ida organization in Iraq. Khyam's claims were corroborated by another cell member, Mohammed Junaid Babar, who became a witness for the prosecution. Babar, a naturalized U.S. citizen who had emigrated from Pakistan as a young child, himself confessed to having attended an al-Qa'ida "summit" meeting held in Pakistan in March 2004 that was devoted to planning international terrorist operations.

Finally, the foiled August 2006 plot to simultaneously bomb ten U.S. airliners and crash them into targets over American cities was de-railed after arrests in Pakistan once more led U.K. and U.S. officials to yet another terrorist cell of British Muslims of Pakistani heritage. That operation's controller was none other than Abu Ubaydah al-Masri: the commander for al-Qa'ida in Kunar Province, Afghanistan. Just as disturbing is the fact that these attacks were not directed against the softer, more accessible targets like subway and commuter trains, hotels and tourist destinations that the conventional wisdom held a de-graded al-Qa'ida only capable of: but against arguably the most internationally-hardened target set since 9/11—commercial aviation. This alarming development calls into question some of our most fundamental assumptions about al-Qa'ida's capabilities and intentions—and indeed our ability to

---

[9] See Honourable House of Commons, Report of the Official Account of the Bombings in London on 7th July 2005, pp. 20–21; and, Robert Winnett and David Leppard, "Leaked No 10 Dossier Reveals Al-Qa'ida's British Recruits," Sunday Times (London), July 10, 2005.

[10] See Intelligence and Security Committee, Report into the London Terrorist Attacks on 7 July 2005, p. 16.

[11] A UK Muslim community leader interviewed in the documentary said that he was approached by Mohammed Khan, who was accompanied by two other British Muslims named Asif Hanif and Omar Khan Sharif, who in 2003 would stage a suicide attack on a seaside pub in Tel Aviv, Israel. See BBC News Media Exchange, "Britain's First Suicide Bombers," "Panorama," broadcast on BBC2 on July 11, 2006, 2000 GMT.

deter them—given that the movement continues to evidence the same grand homicidal ambitions it demonstrated on 9/11.

Rather than solely the product of radicalization then, this concatenation of plots and attacks actually represents the fruition of strategic decisions made by al-Qa'ida a decade ago. As far back as 1999, British authorities already knew of al-Qa'ida's years-long subversive activities among that country's Muslim community: having concluded that some 3,000 British Muslims had left and returned to the United Kingdom during the latter part of the 1990s after receiving terrorist training at al-Qa'ida camps in Afghanistan, Pakistan, Yemen, and elsewhere.[12] The Netherlands' intelligence and security service similarly called attention to increased terrorist recruitment efforts among assimilated Dutch Muslim youths in its 2002 report to the Dutch Parliament. The service detailed the increased terrorist recruitment activities among Muslim youth living in the Netherlands whom it was previously assumed had been completely assimilated into Dutch society and culture.[13] Thus, representatives of Muslim extremist organizations—including, presumably, al-Qa'ida—had succeeded in embedding themselves in, and were already in the process of drawing new sources of support from, receptive elements within established Diaspora communities.

In this way, new recruits could be brought into the movement who would likely had not previously come under the scrutiny of local or national law enforcement agencies. Indeed, according to the aforementioned BBC News documentary, Khan, the 2005 London bombing cell's ringleader, may have acted precisely as such an al-Qa'ida "talent spotter": trawling Britain's Muslim communities during the summer of 2001—literally weeks before 9/11—seeking to attract new recruits to the movement.[14] Finally, senior officials in Spain's Interior Ministry and Foreign Ministry have told me that they now suspect that prior to 9/11 somewhere between a couple hundred and perhaps as many as a thousand Muslims living in Spain similarly were recruited to travel overseas to receive training in al-Qa'ida camps before returning to Spain. The threat, therefore, is not just of jihadi radicalization, but of deliberate, longstanding al-Qa'ida subversion.

This recruitment of locally radicalized individuals into the ranks of al-Qa'ida and other international terrorist organizations has proven more difficult for the authorities in these countries to track, predict and anticipate. Sir David Pepper, the director of Government Communications Headquarters (GCHQ), Britain's equivalent of our National Security Agency (NSA) admitted this in testimony before a House of Commons committee investigating the 7/7 attacks. "We had said before July [2005], there are probably groups out there that we do not know anything about," Sir David explained,

> and because we do not know anything about them we do not know how many there are. What happened in July [viz., the 2005 London bombings] was a demonstration that there were. . .conspiracies going on about which we essentially knew nothing, and that rather sharpens the perception of how big, if I can use [Secretary of Defense Donald] Rumsfeld's term, the unknown unknown was.[15]

These recruits have also proven extremely difficult, if not impossible, for the authorities to effectively profile.[16] Although the members of such terrorist cells may be marginalized individuals working in menial jobs from the lower socio-economic strata of society, some with long criminal records or histories of juvenile delinquency; others may well come from solidly middle and upper-middle class backgrounds with university and perhaps even graduate degrees and prior passions for cars, sports, rock music and other completely secular, material interests. For example, in the case of radicalized British Muslims, since 9/11 we have seen terrorists of South Asian and North African descent as well as those hailing both from the Middle East and Caribbean. They have included lifelong devout Muslims as well as recent converts; persons from the margins of society who made a living as thieves

---

[12] Robert Winnett and David Leppard, "Leaked No 10 Dossier Reveals Al-Qa'ida's British Recruits," Sunday Times (London), July 10, 2005.

[13] See General Intelligence and Security Service, Recruitment for the Jihad in the Netherlands: From Incident to Trend (The Hague: Ministry of the Interior and Kingdom Relations, December 2002).

[14] A UK Muslim community leader interviewed in the documentary said that he was approached by Mohammed Khan, who was accompanied by two other British Muslims named Asif Hanif and Omar Khan Sharif, who in 2003 would stage a suicide attack on a seaside pub in Tel Aviv, Israel. See BBC News Media Exchange, "Britain's First Suicide Bombers," broadcast on BBC2 on July 11, 2006, 2000 GMT.

[15] Quoted in Intelligence and Security Committee, Report into the London Terrorist Attacks on 7 July 2005, pp. 30–31.

[16] The report concluded that "The July attacks emphasized that there was no clear profile of a British Islamist terrorist." See Ibid., p. 29.

or from drug dealing, as well as students from solid middle class and upper-middle class backgrounds who had attended such distinguished British universities as the London School Economics and King's College, London.[17] What they will have in common is a combination of a deep commitment to their faith—sometimes recently rediscovered; an admiration of Bin Laden for the cathartic blow struck against America on 9/11; a hatred of the United States, the United Kingdom and the West; and, a profoundly shared sense of alienation from their host countries. These radicalized individuals are thus readily manipulated, influenced, exploited and then harnessed by al-Qa'ida "talent spotters" for the execution often of suicide terrorist operations. "There appear to be a number of common features to this grooming," the report of the Intelligence and Security Committee of the House of Commons concluded.

> In the early stages, group conversation may be around being a good Muslim and staying away from drugs and crime, with no hint of an extremist agenda. Gradually individuals may be exposed to propaganda about perceived injustices to Muslims across the world with international conflict involving Muslims interpreted as examples of widespread war against Islam; leaders of the Muslim world perceived as corrupt and non–Islamic; with some domestic policies added as 'evidence' of a persecuted Islam; and conspiracy theories abounding. They will then move on to what the extremists claim is religious justification for violent jihad in the Quran and the Hadith. . .and—if suicide attacks are the intention—the importance of martyrdom in demonstrating commitment to Islam and the rewards in Paradise for martyrs; before directly inviting an individual to engage in terrorism. There is little evidence of overt compulsion. The extremists appear rather to rely on the development of individual commitment and group bonding and solidarity [my emphasis].[18]

These new recruits are the anonymous cogs in the worldwide al-Qa'ida enterprise and include both longstanding residents and new immigrants found across Europe, but specifically in countries with large expatriate Muslim populations such as Britain, Spain, France, Germany, Italy, the Netherlands, and Belgium.

Thus, al-Qa'ida's goal remains as it has always been: to inspire radicalized Muslims across the globe to join the movement's holy fight. Not only does al-Qa'ida retain its core operational and command-and-control capabilities, it has shown remarkable resiliency and a stubborn capacity for renewal and regeneration. Even though its personnel may be dispersed, al-Qa'ida remains a hierarchal organization: capable of ordering, planning and implementing bold terrorist strikes. This was precisely the conclusion reached by Senior British intelligence and security officials and publicly stated in October 2006. And, in a speech delivered the following month by Dame Eliza Manningham-Buller, then director-general of the Security Service (MI–5), she was unequivocal in her assessment of the threat posed by al-Qa'ida. "We are aware of numerous plots to kill people and to damage our economy," Dame Eliza stated. "What do I mean by numerous? Five? Ten? No, nearer 30 that we currently know of," she continued. "These plots often have linked back to al-Qa'ida in Pakistan and through those links al-Qa'ida gives guidance and training to its largely British foot soldiers here on an extensive and growing scale."[19] Indeed, al-Qa'ida has been involved in virtually every other major terrorist plot unmasked or actual attack in the United Kingdom since 2003.[20]

---

[17] For instance, in the criminal category are Richard Reid (the so-called "shoe bomber," who attempted to blow up an American Airlines flight en route from Paris to Miami in December 2001) and Jermaine Lindsay (one of the 7/7 London bombers), while Omar Saed Sheikh (who orchestrated the kidnapping and murder of Wall Street Journal reporter Daniel Pearl in 2002) is a graduate of the LSE and Omar Sharif Khan (one of the two British Muslims who carried out a suicide bombing attack against a seaside pub in Tel Aviv, Israel in April 2003) attended the University of London.

[18] Honourable House of Commons, Report of the Official Account of the Bombings in London on 7th July 2005, pp. 31–32.

[19] Quoted in BBC News, "Extracts from MI5 Chief's Speech," November 10, 2006 accessed at http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hl/news/6135000.stm.

[20] These include the so-called "ricin plot" in January 2003 involving an Algerian al-Qa'ida operative named Kamal Bourgass and what British authorities refer to as "Operation Crevice" and "Operation Rhyme," as well as this past summer's abortive plot to crash ten U.S. airliners into American cities. See Elaine Sciolino and Don Van Natta, Jr., "2004 British Raid Sounded Alert on Pakistani Militants," The New York Times, July 14, 2005; and idem., "Europe Confronts Changing Face of Terrorism," The New York Times, August 1, 2005; Sebastian Rotella, "British Terrorism Case Parallels Others; Trial in a suspected plot to bomb a nightclub or mall in 2004 involves alleged home-grown Islamic radicals with ties to militants in Pakistan," Los Angeles Times, September 1, 2006; and BBC News, "Man Admits UK–US Terror Bomb Plot," October 12, 2006 accessed at http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk—news/6044.

CONCLUDING REMARKS: A WAY AHEAD?

Al-Qa'ida may be compared to the archetypal shark in the water that must keep moving forward—no matter how slowly or incrementally—or die. In al-Qa'ida's context, this means adapting and adjusting to even our most consequential countermeasures while simultaneously searching to identify new targets and vulnerabilities and continuing to replenish its ranks with new recruits as well as sympathizers and supporters. In sum, Qa'ida's capacity to continue to prosecute this struggle is also a direct reflection of both the movement's resiliency and the continued resonance of its ideology and effectiveness of its communications.

Defeating al-Qa'ida suggests first and foremost that our assessments and analyses must be anchored firmly to sound empirical judgment and not blinded by conjecture, mirror-imaging, politically partisan prisms and wishful thinking. Second is the need to refocus our attention and efforts back to South Asia—to Pakistan and Afghanistan, specifically—where it was following 9/11 and when al-Qa'ida was indeed on the run. Third is the recognition that al-Qa'ida cannot be defeated with military means alone. As one U.S. intelligence officer with vast experience in this realm told me over two years ago: "We just don't have enough bullets to kill them all." Accordingly, a new strategy and new approach is needed given a resuscitated al'Qa'ida organization that relies as much upon clandestine subversion of targeted communities as it does upon propaganda and radicalization. Its success will depend on effectively combining the tactical elements of systematically destroying and weakening enemy capabilities alongside the equally critical, broader strategic imperatives of countering the continued resonance of the movement's message and breaking the cycle of terrorist recruitment and replenishment that has both sustained and replenished al-Qa'ida.

The war on terrorism has now lasted longer than America's involvement in World War II. Yet, even today we cannot claim with any credibility, much less, acuity to have fulfilled Sun Tzu's timeless admonition.[21] Indeed, what remains missing six years since this war began is a thorough, systematic understanding of our enemy: encompassing motivation as well as mindset, decision-making processes as well as command-and-control relationships; and ideological constructs as well as organizational dynamics.

Forty years ago, the United States understood the importance of building this foundation in order to effectively counter an enigmatic, unseen enemy motivated by a powerful ideology who also used terrorism and insurgency to advance his cause and rally popular support. Although America, of course, encountered many frustrations during the Vietnam conflict, a lack of understanding of our adversary was not among them. Indeed, as early as 1965, the Pentagon had begun a program to analyze Vietcong morale and motivation based on detailed interviews conducted among thousands of guerrilla detainees. These voluminously detailed studies provided a roadmap of the ideological and psychological mindset of that enemy, clearly illuminating the critical need to win what was then often termed the "other war"—the ideological struggle for the hearts and minds of the Vietnamese people.[22] Even if the fundamental changes required in U.S. military strategy to overcome the Vietcong's appeal went ignored, tremendous effort and resources were devoted to understanding the enemy.

Today, Washington has no such program in the war on terrorism. America's counterterrorism strategy continues to assume that America's contemporary enemies—be they al-Qa'ida or the insurgents in Iraq—have a traditional center of gravity. It also assumes that these enemies simply need to be killed or imprisoned so that global terrorism or the Iraqi insurgency will both end. Accordingly, the attention of the U.S. military and intelligence community is directed almost uniformly towards hunting down militant leaders or protecting U.S. forces—not toward understanding the enemy we now face. This is a monumental failing not only because decapitation strategies have rarely worked in countering mass mobilization terrorist

---

[21] I have been making this same argument since I testified on this same issue before Congress in 2005. See, for instance, Bruce Hoffman, Combating Al-Qa'ida and the Militant Islamic Threat (Santa Monica, CA: RAND Corporation, CT–255, 2006, 2005) available at http://www.rand.org/pubs/testimonies/CT255.

[22] The RAND Corporation actively contributed to these analyses in a series of detailed reports, based on voluminous interviews of captured Vietcong. See, for example: Leon Gouré, Anthony Russo, and D. Scott, Some Findings of the Viet Cong Motivation and Morale Study: June—December 1965 (Santa Monica, CA: RAND, RM–4911–12–ISA/ARPA, February 1966); Leon Gouŕ, J. M. Carrier, and D. Scott, Some Findings of the Viet Cong Motivation and Morale Study: January–June 1966 (Santa Monica, CA: RAND, RM–5137–ISA/ARPA, February 1966); J. M. and Charles Thomson, Viet Cong Motivation and Morale: The Special Case of Chieu Hoi (Santa Monica, CA: RAND, RM–4830–2–ISA/ARPA, May 1966); J. C. Connell, Viet Cong Motivation and Morale: A Preliminary Report (Santa Monica, CA: RAND, RM–4507/2–ISA, July 1968).

or insurgent campaigns, but also because al-Qa'ida's ability to continue this struggle is ineluctably predicated on its capacity to attract new recruits and replenish its resources.

The success of U.S. strategy will therefore ultimately depend on Washington's ability to counter al-Qa'ida's ideological appeal and thus effectively address the three key elements of al-Qa'ida's strategy:

- the continued resonance of their message;
- their continued ability to attract recruits to replenish their ranks; and,
- their stubborn capacity for continual regeneration and renewal.

To do so, we first need to better understand the mindset and minutia of the al-Qa'ida movement, the animosity and arguments that underpin it and indeed the regions of the world from which its struggle emanated and upon which its hungry gaze still rests. Without knowing our enemy we cannot successfully penetrate their cells; we cannot knowledgeably sow discord and dissension in their ranks and thus weaken them from within; we cannot effectively counter their propaganda and messages of hate and clarion calls to violence; and, we cannot fulfill the most basic requirements of an effective counterterrorist strategy: preempting and preventing terrorist operations and deterring their attacks. Until we recognize the importance of this vital prerequisite, America will remain perennially on the defensive: inherently reactive rather than proactive, deprived of the capacity to recognize, much less anticipate, important changes in our enemy's modus operandi, recruitment and targeting.

Ms. HARMAN. Thank you very much.

Ms. Katz, you are now recognized for 5 minutes.

STATEMENT OF RITA KATZ, DIRECTOR, SITE INSTITUTE

Ms. KATZ. Thank you, Madam Chair, and all the members of this community for allowing me to offer some of my analyses in studying the Internet jihadist community.

Since the war on terror began after 9/11, the United States and the West have embarked and campaigned against al-Qa'ida. Yet, anyone who reads the front page of the newspaper today can see that al-Qa'ida and other jihadist groups are far from defeated, and occasionally people from our own society are arrested for plotting to carry out domestic attacks.

Despite being isolated and hunted, the leaders of the jihadist groups nevertheless maintain an active dialogue with their followers, issuing statements through the Internet to a worldwide audience.

Jihadists continue to hold al-Qa'ida in the highest esteem, with localized terrorist groups in Iraq, Egypt, Algeria, Somalia, Libya and elsewhere, pledging their allegiance to bin Laden and his organization.

Post 9/11, terrorist bombings in Madrid, London, Bali, Istanbul and elsewhere demonstrate that the war on terror is not won. It seems, though, as a never ending series of terrorist plots and training camps are constantly being broken up across the world from China to Canada. Despite very real and significant success, dismantling and disrupting terrorists and their supporters, the terrorist threat remains and does not appear to be shrinking. Jihadist networks have evolved to a point where no gun, bomb or assassination can harm them permanently.

One of the primary sources of jihadist resilience is the Internet. It is the Internet that enables jihadist networks to continue to exist despite the almost unlimited resources that the United States has dedicated to the war on terror. Though guns, IEDs and other weapons are necessary for terrorists to remain dangerous, the Internet is what enables them to coordinate, share information, recruit new

members and propagate their ideology. If we do not treat the Internet as a crucial battleground in the war on terror, we will not be able to defeat the jihadist threat.

The virtual jihadist network has replaced al-Qa'ida training camps. As someone who lives within the jihadist community and spends most of my day with the jihadists, I must say that it is easy for me to understand how for a jihadist it is one of the most addictive, interactive and informative experiences that fulfills the social needs of each and every one of them.

From video games to making bombs to religious justifications to friendships, each jihadist feels as he is part of a greater connected community. This overwhelming and gratifying experience for the jihadist explains why members of these online forums are suddenly announced as being dead as a result of carrying out a suicide operation in Iraq, Afghanistan or elsewhere. The joy and the pleasure the online jihadists share in celebrating such a death is stunning.

Though the online jihadist network has benefited the global jihadist movement, at the same time it has provided us with an open window into the means and methods by which jihadist groups operate today. By studying the various dimensions of the virtual jihadist network and then infiltrating them, we can learn about our enemy, including their mindset, who they are, their location, their ideology, trends and tactics. Understanding our enemy will help us to counter their propaganda, predict types of future attacks, find them and defend ourselves against their methods.

In my submitted statement, I outlined in detail how the online jihadist movement is currently structured, including how jihadist groups are organized online, how information is being disseminated, how new members are being recruited and how the jihadist groups like al-Qa'ida communicate among themselves and with their followers all through the Internet.

As long as the Internet remains a safe haven for jihadists, uncontested by the law enforcement agencies, the jihadist movement will continue to grow even after its leaders are killed. The challenge is to infiltrate and erode this virtual network. Studying the online jihadist community empowers us. We can listen to what they say, understand the way they think. We can better defend ourselves.

SITE has repeatedly implemented such techniques and was able to provide intelligence agencies with information that led to apprehension of would-be terrorists and suicide bombers.

In closing, I hope that you all recognize the importance of the Internet. And that is why we are here today. Thank you very much.

[The statement of Ms. Katz follows:]

PREPARED STATEMENT BY RITA KATZ, DIRECTOR, SITE INSTITUTE, AND JOSH DEVON, SENIOR ANALYST SITE INSTITUTE

The Internet: The Most Vital Tool for Terrorist Networks

More than six years after 9/11, the United States has done little to contest jihadists' use of the internet, arguably one of the most crucial tool that enables modern terrorist networks to exist. Jihadists use the internet to recruit, coordinate, communicate, raise financing, plot attacks, and even as a social network. Yet, after much interaction with government officials from several agencies, including the military as well as domestic law enforcement, it is clear that while the government understands that the internet is being used by jihadists, few steps have been made

to to study this phenomenon. It is clear by the ballooning influence of the internet in fostering a global insurgency against the West and its interests, the government lacks a full grasp of how jihadists exploit the internet, and even less of an idea on how to combat this threat effectively in a coordinated effort.

Today, there are tens of thousands of members on the half a dozen most important and exclusive online password-protected jihadist messageboards, and many more in line to take the place of those members who have used the internet to pave the way to kill themselves in suicide bombings in Iraq, Afghanistan, Somalia, Chechnya, and Lebanon. Likewise, as it has become more difficult to travel to current conflict areas for military instruction, the internet provides a virtual training camp for those members who seek to plan homegrown terrorist attacks in the United States and other Western targets. It is the internet that enables jihadist groups to foster a global insurgency, preparing like-minded individuals all over the world with the necessary military, technical, and social skills to produce a dangerous, united movement aimed at harming the West and Western interests.

Though labyrinthine, confusing, and requiring the in-depth study of complex social and technical networks, this essential battleground in combating the terrorist threat must be considered as important as fighting terrorists on the ground. Attempted homegrown terrorist attacks on the West have increasingly included an online component, whether the assailants were using the internet to coordinate the transfer of information, download military manuals, watch jihadist videos, or participate on jihadist messageboards. Of course, guns, IEDs, and other weapons are necessary for terrorists to maintain their relevance and dangerousness, but the internet is what enables jihadists to coordinate attacks, share information, recruit new members, and propagate their ideology. There is no longer any doubt that the internet is the heart of the global jihadist movement.

The government has attempted to monitor the internet by automatically analyzing huge amounts of online traffic through computers, which has led to positive results intercepting emails and other online communication related to terrorist activity. However, this method of data gathering misses crucial intelligence, especially as jihadists come up with novel ways to avoid automated detection online, and glosses over the critical nuances that comprise the online jihadist community, like their demographics, their geography, their ideology, and their manner of thinking.

As the SITE Institute and other private organizations have successfully been able to gather actionable intelligence from jihadists on the internet, not by using supercomputers but instead by knowing where and when to look, after having spent several years infiltrating, studying, and analyzing the online jihadist community. As just one example, after infiltrating and monitoring an online jihadist internet forum used for recruitment, the SITE Institute obtained intelligence that members of the forum were soon leaving their countries of residence in Europe to engage in suicide operations against coalition forces in conflict areas. The SITE Institute first alerted domestic law enforcement, who were unaware of the threat, and then contacted law enforcement officials in Europe, who determined that the intelligence was indeed actionable and promptly detained the individuals. This case, and others like it, are representative of how law enforcement agencies, in the United States and Europe, are not sufficiently monitoring the internet effectively.

Though necessary, rather than just using software to analyze massive flows of data hoping that a jihadist will use a key word like "bomb" in an email, the government also needs to focus its efforts on the much more difficult task of studying people to understand our enemy. This initiative involves a radical retraining of government analysts, who must at the same time be able to interpret and understand server logs, PHP, networks of IP addresses, and databases, in addition to a deep knowledge of jihadist culture and history, as well as foreign languages like Arabic, Turkish, Urdu, and Pashtu. Without the combination of these skills, which is what our enemies already possess, the United States will not be properly equipped to combat jihadists on the internet.

However, if the U.S. does cultivate these skills, it can deal severe blows to the global jihadist community. By effectively studying the internet, law enforcement and the military can learn about our enemy, including who they are, their location, their ideology, trends in tactics, and what training they are receiving. Understanding our enemy will help to counter their propaganda, predict types of future attacks, find them, and defend ourselves against their methods. Whether fighting groups of jihadists in Iraq or self-indoctrinated, homegrown terrorists in the United States, focusing on the internet puts law enforcement in the best possible position to combat the global jihadist threat.

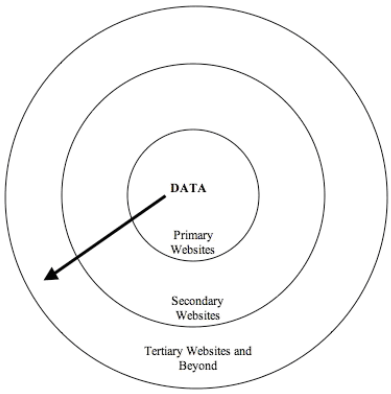
Current Structure of the Online Jihadist Movement

In order to understand the global jihadist threat, it is necessary to review the structure of the online jihadist movement. After developing a basic knowledge of how jihadists groups utilize the internet, one can see how established jihadist groups like al-Qa'ida direct the jihadist movement and can continue to exist despite the traditional measures taken against them. Once dissected, the online jihadist movement can be infiltrated, analyzed, and countered. The following provides an overview of how jihadists uses the internet, how information is disseminated and circulated, and how the internet serves all the necessary functions jihadist groups need to continue to survive.

At least since the 1990s, Al-Qa'ida and other jihadist groups have used the internet to broadcast propaganda and recruit members. After 9/11 and the resulting destruction of terrorist training camps followed by the ensuing decentralization of al-Qa'ida and other jihadist groups, the internet became essential to allowing jihadist groups to continue to operate effectively. Today, jihadist groups utilize websites, messageboards,[1] e-groups, blogs, instant messaging, and other services available through the internet to continue to indoctrinate, communicate, recruit, and plan attacks.

While many may perceive that jihadist activity on the internet is chaotic, it is in fact very structured. Only a handful of primary source jihadist websites distribute the media of the leaders of al-Qa'ida and other jihadist groups. Through this small number of specific, password-protected online forums, the leading jihadist groups, like al-Qa'ida, post their communiqués and propaganda. By keeping the number of primary source jihadist websites small, online jihadist ideologues and leaders of jihadist groups can provide a transparent mechanism to authenticate communiqués. In this way, the global jihadist movement can instantly discern the difference between official and fake communiqués by checking the source of the website and the individual who posted it. Though the number of primary source forums is small, there are tens of thousands of members registered on these websites, giving the jihadists a wide reach.

Once an official message from a jihadist group is posted to a primary source message forum, members of the primary message forum will then disseminate that posting to other secondary messageboards. From these secondary messageboards, other peripheral individuals will then disseminate the information onto other messageboards (See Figure Below)



issemination of Primary Source Jihadist Data

Thus, the online jihadist movement has developed in such a way that it is at once decentralized but rigidly hierarchical. The jihadists can demonstrate that their communiqués are authentic by releasing information only on the primary websites and then rely on the secondary and tertiary websites to disseminate their data to larger groups of people.

[1] An online messageboard, also called an online forum, allows users to communicate and discuss topics easily with each other on the same website. Messageboards, which may be password-protected, foster the creation of virtual communities and are essential to reinforcing a shared global jihadist identify.

Al-Fajr Center

The group that coordinates the online distribution of authentic jihadist communiqués, such as a video by bin Laden, Zawahiri, and other jihadist leaders, is called Al-Fajr Center. Established officially in January 2006, Al-Fajr Center is entirely virtual and exists only online. The organization serves not only al-Qa'ida but numerous jihadist groups who share the same ideology. Besides al-Qa'ida, the groups that utilize Al-Fajr Center include several of the Iraqi insurgency groups, Palestinian jihadist groups, Al-Qa'ida in the Islamic Maghreb (formerly the GSPC), the Libyan Islamic Fighting Group, Somali jihadist groups, Saudi jihadist groups, the Taliban and other insurgent groups in Afghanistan, and even a group in western China.

The underlying purpose of Al-Fajr Center is to coordinate propaganda efforts through highly centralized and secure channels. This enables the groups utilizing al-Fajr to unify strategies, achieve economies of scale, and establish trusted channels of communication. Through the center's efforts, individuals across the globe are provided with easy access to authentic jihadist propaganda coming from a single source. This tactic slowly erases the lines between the regional terrorist groups, effectively portraying a strong, united group against the West. Because of the apparent closeness between al-Qa'ida and the other groups using Al-Fajr Center, those indoctrinated by Al-Fajr Center will support any jihadist group releasing media through the center, not just al-Qa'ida.

The group's products are eclectic and very frequent, creating a stimulating environment for jihadists. Al-Fajr Center distributes dozens of daily communiqus from jihadist groups taking credit for attacks in Iraq, Afghanistan, Algeria, and elsewhere. In addition to these daily communiqués, the group also regularly dispatches special releases. For example, in November 2006, Al-Fajr released a written analysis of the current state of conflict in Afghanistan. The following week, the organization released a strategic manual, the "Technical Mujahid," devoted to understanding the internet and internet security. The very next day, the center was responsible for the release of a video provided by a representative of a Somali jihadist group. These releases came only days after a video calling for jihad in Xinjiang, China, called East Turkistan by the jihadists.

Al-Fajr Center itself is very structured and is divided into several different brigades, each with a designated purpose.

These brigades include:

- **Hacking Brigade,** in charge of hacking websites, carrying out Denial of Service (DoS) attacks, and identifying vulnerable websites
- **Intelligence Brigade,** in charge of gathering information, both online and in the physical world. For example, this brigade monitors the websites of the government, think tanks, and the media, like the White House, the U.S. Army, the Rand Corporation, the Jamestown foundation, Newsweek, Time Magazine, and others.
- **Distribution Brigade,** in charge of distributing the propaganda released by jihadist groups, such as taking credit for daily attacks, media from jihadist leaders, videos of attacks, training videos, and other videos of fighting from all over the world
- **Publications Brigade,** in charge of producing studies and training manuals in magazine form, like the "Technical Mujahid"
- **Cybersecurity Brigade,** in charge of protecting the security of jihadist websites
- **Multimedia Brigade,** in charge of producing multimedia jihadist propaganda, including attacks on American forces, preparation of IEDS, audio and video messages from jihadist leadership, statements of martyrs, and other propaganda

Each of these groups has its own special messageboard which only members of each brigade can access. Each brigade contains leaders who coordinate their efforts with the jihadist leadership. The costs to run these brigades are minimal, as those involved are donating their time and effort for their cause. The members of these brigades do their work not for any particular jihadist group but for the entire movement. The virtual layer between the members of these brigades and the actual jihadist groups themselves creates an extremely operationally secure mechanism to transmit information.

While these propaganda efforts are the driving force behind Al-Fajr Center, the organization does serve another purpose for jihadist groups by providing numerous services for jihadist leaders. Because Al-Fajr Center is in communication with representatives of all the major jihadist groups, including al-Qa'ida, it can also facilitate the rapid transfer of information between jihadist groups and pass on information that the center has gathered. In this way, the online representatives of jihadist

groups can then pass the information on to the leaders of there groups via courier, even in the remote areas of the Northwest Frontier Province in Pakistan.

This mechanism may help explain how isolated jihadists like bin Laden and Zawahiri can reference extremely current events in the propaganda they release. Likewise, the efficiency of Al-Fajr Center may also explain how jihadist leaders have been able to release messages more frequently than in the past. Reinforcing this trend is that jihadist leaders have begun to release their videos online first, rather than relying on the al-Jazeera television network, which often only shows a small portion of the entire propaganda piece.

Al-Fajr Center is a powerful tool for jihadist groups because their messages can be spread rapidly while retaining their authenticity. As the primary outlet for most of the major jihadist groups, Al-Fajr Center's operations contribute greatly to fostering a unified, global jihadist community. Similarly, the center benefits jihadist groups themselves by allowing them to coordinate, share information, and consolidate their power to continue to lead the jihadist movement. Damaging Al-Fajr Center would prove a severe blow to the jihadist groups' ability to gather information, proselytize, and recruit.

From Propaganda Groups to Terrorist Facilitators

While some may think that propaganda groups like Al-Fajr Center are not an immediate threat because they only release propaganda on the internet, the reality is that the propaganda groups themselves facilitate terrorist activity. A case in point is the Global Islamic Media Front (GIMF), one of the oldest and most prominent virtual propaganda groups. The GIMF, which also disseminates its propaganda through Al-Fajr Center, is just one of many virtual groups who contribute propaganda to the online jihadist community. Some groups, like GIMF, do not work for any one particular jihadist organization but are instead made up of supporters who believe in the jihadist ideology and support the general movement. The existence of these groups provides the online jihadist with a continuous stream of propaganda, never leaving the online jihadist community without movies, documents, messages, magazines, training manuals, and even video games, all of which are created to indoctrinate others to support the jihadist cause.

GIMF, which openly supports al-Qa'ida, produces copious amounts of propaganda maintains a hidden membership of individuals scattered throughout the world. These ardently dedicated individuals produce a wide variety of jihadist propaganda in the form of Flash presentations, videos,online televisions news, and even video games. One of GIMF's most popular video games was titled "Night of Bush Capturing." The first-person perspective shooting game, in which the player targets American soldiers, President George Bush, Prime Minister Tony Blair, and Grand Ayatollah Ali Al-Sistani, was distributed in September 2006 throughout jihadist message boards and created for "terrorist children."

However, GIMF's activities were not limited to propaganda; instead, many of its members plotted terrorist attacks themselves, using the virtual network they had built to facilitate its actions. In the summer of 2007, Mohammad Mahmoud, a leading member of GIMF living in Vienna, Austria, worked closely with Jeish al-Islam, the Palestinian jihadist group responsible for the kidnapping of BBC journalist Alan Johnston in the Gaza Strip. In this case, Mahmoud used his online network to help the terrorist group issue statements and parade the powerful symbol of a Western hostage.

Soon, however, Mahmoud took further steps to help others plan attacks. Known on the internet as "Gharib al-Diyar," Mahmoud ran the German-branch of GIMF, but did not limit himself to propaganda only. In 2003, he travelled to Iraq to attend a training camp run by Ansar al-Islam, a jihadist group currently active in Iraq under the name Ansar al-Sunnah. After producing a March 2007 GIMF video speech threatening attacks in Germany and Austria, Mahmoud composed a rough message outlining several physical targets to attack, specifically the Euro 2008 football championships in Austria and Switzerland, OPEC's Vienna-based headquarters, as well as UN buildings in Vienna and Geneva.

In September 2007, officials in Vienna arrested Mahmoud and two of his associates, while a coordinated arrest took place outside Montreal, Quebec, in which Canadian officials arrested Said Namouh. According to a charge sheet filed in Quebec, Namouh conspired with Mahmoud "for the purpose of delivering, placing, discharging or detonating an explosive in a place outside Canada." Using the name "Achrafe" on the internet, Namouh was also an important member of GIMF, sending hundreds of messages to other members of the group all over the world. Notably, the internet enabled Mahmoud to provide Namouh with the alleged support to plan a terrorist attack while across the Atlantic Ocean.

As this example demonstrates, jihadist propaganda groups must also be treated as potential terrorist cells. This GIMF case is but one example of many other cases where those facilitating propaganda seek to support actual attacks. Indeed, instructional manuals produced by virtual jihadist groups like GIMF now encourage individual jihadists and jihadist groups to train as multi-faceted operators, learning both the production and dissemination of media propaganda in addition to the technical operations required to carry out attacks. As this trend continues, it becomes increasingly dangerous to view individuals involved in jihadist propaganda as disconnected from those seeking to carry out attacks. It is therefore extremely important that we closely monitor virtual jihadist groups, no matter how small, to learn as much as we can about them and their activities before they are able to cause harm.

The Virtual Jihadist Network

Jihadist groups use the internet to provide a virtual social network to indoctrinate, recruit, and train followers. Because of the constant and overwhelming propaganda the jihadists produce, any individual, even with no prior association to jihadist ideology, can quickly feel like he or she is part of the global jihadist community and self-radicalize himself or herself. Once a believer, these self-radicalized individuals will seek out others who think like them online, eventually discovering the primary source jihadist websites run by the jihadists themselves. By studying these primary source websites, jihadist groups can cull new recruits while exerting much less effort, as potential recruits come to them, rather than the opposite.

In addition, through this virtual jihadist network, jihadist groups can indoctrinate individuals and them provide them with the tools they need to carry out either individual or small group attacks, without having to be specifically recruited by an established jihadist group. Jihadists provide strategies and tactics for the entire community so that independent terrorist cells can spring up throughout the world. From online training manuals, these independent cells can learn which are the best targets to attack, how to attack them, and how to make sure that the attack will be inline with the overall jihadist strategy.

The virtual jihadist network revolves around these dimensions:

- Recruitment
- Propaganda, Indoctrination, and Psychological Warfare
- Training and Tactics
- Communication and Coordination
- Strategy
- Financing

The following will examine each dimension of the virtual social network in further detail.

Recruitment

Recruitment takes on two forms in the online jihadist community. The first path is attempting to head to a current theater of conflict to fight with the mujahideen. These recruits are sometimes required to bring money with them to support the jihad. Though many jihadists likely utilize local connections to make their way to the lands of jihad, online handlers also exist to aid jihadists wishing to travel to an area where they can fight. Mark Robert Walker, a 19-year-old student in Laramie, Wyoming, originally from Rochester, New York, pled guilty to aiding a terrorist organization in October 2005. Using the screen name "Abdullah," Walker was in contact with an online individual named "Khalid" who had agreed to help Walker leave the United States to fight with jihadists in Somalia. The FBI intercepted Walker's online communications with "Khalid" and arrested Walker at El Paso International Airport, as he attempted to leave the country.

Walker's case is not isolated; many like him exist within the online community. These members who desire to travel to lands of jihad to fight with the mujahideen are reinforced by the material found on the forums. Jihadist messageboards proudly announce when a member of a forum has been killed while fighting. On February 6, 2007, the al-Hesbah jihadist forum carried a message announcing that one of its members had carried out a successful suicide attack in Iraq that "shook the crusaders" in Iraq. The individual, an established jihadist online figure known by the alias "Risalah," died while fighting since the start of 2007. On January 3rd, 2007, Na'im Muhammad bin Abdullah, also a member, was announced to have been killed fighting U.S. forces in Baghdad. Both were prominent members of the online jihadist community. The announcements of their deaths prompted praise from other members, reinforcing the strength of the community. This praise also paints physical jihad as a natural outgrowth of participation in the online forum.

Al-Hesbah is not the only jihadist forum with members who have left to join the jihad. For example, after a Saudi administrator of the Hedayah forum[2] was killed fighting in Iraq in December 2006, one member eulogized him, "In the forum he was special and was a provider. . .and there he is today, writing. . .with his blood, not with his pen." Just traveling to a land of jihad garners praise, as well. In December 2006, it was announced that Firas al-Ta'an, a moderator of Al-Ekhlaas[3] jihadist forum, had traveled to Iraq and reached the mujahideen safely.

Rather than travel to where there is active fighting, the other path a recruit can take is to engage in a local terrorist plot, where no handler is needed. Instead, the training manuals, tactics, and strategies available within the online jihadist community take the place of a handler. For example, in March 2004, Mohammad Zaki Amawi, a US citizen, returned to Ohio after a failed attempt to enter Iraq through Jordan to fight against US and coalition forces. Undeterred by his inability join an active front, Amawi gather jihadist training manuals and videos through jihadist websites to build his own cell in Toledo. He soon recruited others local to the area.

Among the materials Amawi collected from online sources to train the cell were a "Basic Training" course for jihadists, a prerequisite for an "Advanced Training" course, videos on the production and use of improvised explosive devices (IEDs), and an instructional video for building a suicide bomb vest, titled "Martyrdom Operation Vest Preparation." One member of the cell, Marwan Othman El-Hindi, proposed downloading the videos to show to two of his recruits in Chicago. For practice, the cell traveled together to a shooting range in Toledo. During this time, Amawi maintained contact with jihadists traveling into and out of Iraq using encrypted e-mail messages, contacting them for technical assistance.

These self-starting cells can also span continents. While in England, Younis Tsouli, the online jihadist known as Irhabi007, was in contact with two men from Atlanta, Georgia, who were providing Irhabi007 with surveillance videos of American targets. The men, Ehsanul Islam Sadequee and Syed Haris Ahmed, visited Washington, DC, and recorded video footage of the U.S Capitol, the Masonic Temple, the World Bank, and a fuel depot. Their footage was found amongst Irhabi007's belongings.

This cell, however, also had another component connected through the internet. In June 2006, Canadian authorities disrupted the cell in Ontario, arresting 17 individuals, including 5 minors. Many members of this cell are charged with attempting to blow up targets throughout Canada. It was soon revealed that the two Georgian men providing support to Irhabi007 had traveled to Canada to meet with members of the cell, after having met online. The men from Georgia were also members of the same jihadist messageboard as some of the members of an alleged cell in Canada.

Jihadists will continue to utilize the internet to recruit others to plan attacks so long as the internet remains a safe haven. Recruitment takes place on jihadist forums in many languages, from Arabic to German to English. By infiltrating the jihadists' online forums, we can better monitor the relationships between online jihadists, looking for both those who wish to travel to lands of jihad as well as those seeking to do harm locally. Studying messageboards allows us to determine which online jihadists participate in the recruiting process and enables us to develop countermeasures to act against them. Furthermore, identifying the physical locations of online jihadists can disrupt actual cells and prevent actual attacks.

Propaganda, Indoctrination, and Psychological Warfare

The propaganda the jihadists release is powerful and reaches a global audience. As one jihadist recalled, "The first time I saw an al-Qa'ida video, I was ready to go. I wanted to kill the disbelievers."[4] The propaganda in jihadist videos is compelling, convincing, and able to be accessed in a growing number of languages. While most primary source propaganda is released in Arabic, individuals and groups dedicated to the jihadist cause will translate them into their vernacular language, so that the message of jihadist leaders can be heard across the world.

Jihadist propaganda is released in English, Turkish, French, Somali, Russian, and a host of other languages. Jihadist messageboards and websites also exist exclusively in English and other languages as well. Even some extremely prominent Arabic jihadist messageboards, like the Al-Hesbah[5] forum, now contain an English section. Because of the availability of jihadist propaganda in so many languages, potential jihadists can know only their native language and still be radicalized.

---

[2] http://www.hedaaya.net
[3] http://www.alekhlaas.net/
[4] Stewart Bell. "Making of a Zealot." *National Post.* June 30, 2006.
[5] http://www.alhesbah.org

By being able to reach a global audience, jihadist groups can continue to indoctrinate many more individuals than they could otherwise without a propaganda outlet through the internet. In an interview released in December 2005, Zawahiri explicitly discussed al-Qa'ida's policy of distributing important videos and messages as widely as possible. At the conclusion of the 43 minute interview, Zawahiri calls upon media organizations to distribute the interview in "all languages and as widely as possible." The release of the interview itself carried English subtitles and was distributed shortly thereafter with French, German, and Italian subtitles on online forums by December 2005.

In the last year, al-Qa'ida's production company, As-Sahab, has begun to produce English transcripts and subtitles for most of al-Qa'ida's major releases, especially messages from bin Laden and Zawahiri. In the past year, at least 20 videos from As-Sahab have been released with either English subtitles or transcripts, broadening the group's reach. Al-Qa'ida has also issued videos in English speaking directly to Americans. A native Californian wanted by the FBI for his role in al-Qa'ida, Adam Gadahn, or Azzam al-Amriki, provides a voice directly from the al-Qa'ida leadership in Afghanistan to the American people. His September 2006 video, "An Invitation to Islam," carried the messages of al-Qa'ida but in an American accent. Gadahn devoted much of his 45 minute video to explaining al-Qa'ida's ideology, rationale, and motivations.

While Adam Gadahn speaks to an American audience, al-Qa'ida uses the British men who perpetrated the July 7, 2005, bombings in London. In commemoration of the bombings, an annual video is released to the forums in which one of the bombers discusses his reasons for the attack in a thick Yorkshire accent. As with "An Invitation to Islam," each of the 7/7 commemoration videos are edited as compilations combining clips of al-Qa'ida leadership with a significant portion read by a native speaker to the people of the country being addressed.

The demand for jihadist materials in other languages is high. Recently, an influential French jihadist forums, al-Mourabitoune,[6] has begun providing translations of videos and statements of responsibility from Arabic into French with very little lag time. For example, on May 23, 2006, GIMF released bin Laden's "A Testimony to the Truth" with both Arabic and English transcripts. By the next day, al-Mourabitoune was carrying a French translation of the transcript. Following a flood of requests posted to English and French messageboards, GIMF provided subtitled editions of Abu Musab al-Zarqawi's April 26, 2006, video, entitled, "A Message to the People." A version of "A Message to the People" with French subtitles was soon released along with a full French transcript to French-language jihadist forums on May 4, 2006.

While many may perceive jihadist propaganda as crude and barbaric, replete with beheadings and bombs, much propaganda is instead strongly argued rhetoric that is becoming increasingly sophisticated. Jihadist ideologues, like Hamid Al-Ali in Kuwait, release masterful pieces of religious rhetoric exhorting others to jihad. Many of the white papers, studies, books, and other documents that the jihadists release are heavily footnoted and maintain a scholarly tone. The result is that the propaganda takes on an air of professionalism and scholarship that is extremely convincing to critically thinking potential jihadists.

Oftentimes jihadist ideologues appeal to baser emotional responses to violence and sex. Abu Musab al-Zarqawi's filmed beheadings attracted an instant audience, and videos are released daily of attacks, gruesome shots of dead victims and mujahideen, and other gore. This gore serves as powerful psychological warfare, and sensationalized murders, like beheadings, intimidate the enemies of the jihadists while bolstering jihadist support. On the other hand, the death of mujahideen is portrayed as painless, desensitizing many to the fear of participating in such violence.

While not commonly addressed, sometimes sex is exploited to attract jihadists. In November 2006, a three and a half minute audio message from Hamid Al-Ali, an extremely important jihadist shaykh famous for his fatwas and designated a terrorist by the United States, was posted to jihadist messageboards explaining the great rewards in heaven waiting for those who die in battle. The speaker provides strikingly erotic details about the "wives" which pleasure martyrs in paradise:

> "Paradise has eight great gates through which whoever enters will never come out again. Each gate determines what the martyr has achieved; in Paradise they will enjoy endless tasteful food and drinks, with a beloved wife. She will astonish your mind. Her hair is made of silk. Her flirtation appears in the bed as politeness and expertise in these things; she knows all about sexual intercourse. By touching, looking, and hearing, her vagina never complains about

[6] http://www.ribaat.org

how much sex she had. She becomes a beautiful virgin again. The more intercourse she has the more love she gives, and she gives a beautiful smile."[7]

The amount of propaganda the jihadists produce is staggering. With jihadist propaganda widely available in numerous languages, the jihadists can reach an extremely large audience. This large reach of jihadist propaganda, coupled with the shrewd use of rhetoric, has created an online jihadist environment where individuals are capable of self-radicalizing themselves with little direct guidance from established jihadist groups. So long as this propaganda is not countered, jihadists will always have a steady stream of potential recruits.

Training and Tactics

Using the internet, jihadists have created a virtual classroom that teaches the online jihadist community how to produce and construct weapons ranging from simple IEDs to nuclear, biological, and chemical weapons. Not only are jihadists taught military tactics; they also learn how to mine the internet for information, protect their anonymity online, encrypt the contents of their computers, and use the internet to benefit the global jihadist movement. Given the difficulty many individuals have in reaching training camps in the post-9/11 world, online training gives jihadists the tools they need to plan, coordinate, and execute terrorist attacks. Indeed, soldiers from Iraq have informed us that training manuals discovered in jihadist safe houses in Iraq were printed from the jihadist manuals found online.

Al-Qa'ida and other jihadist groups have produced magazines and multimedia exclusively for training purposes. "Al-Battar," a publication of al-Qa'ida in Saudi Arabia, is solely dedicated to training prospective mujahideen, even supplying ideal targets. Issues have featured weapons discussion, such as using a pistol for sniper training, how to hold and target a rocket-propelled grenade (RPG), and survival tactics. Even though the most recent issue of "Al-Battar" was released two years ago, the magazine continues to widely circulate online on jihadist websites.

Excerpts from large compendiums of urban warfare, explosives and poisons training manuals are frequently posted to the jihadist forums, in addition to members own suggestions, often using photographs and video to support their explanations. Videos exist which give training instructions for suicide bombings, construction and dismantling of landmines, and composition of various explosives substances. Electronic books, or e-books, are also used to provide a single resource for particular training. For example, an e-book compilation of IED construction, camouflage, and placement was distributed to the password-protected al-Firdaws[8] forum, which contains a special military section. This publication suggested the planting of explosives in shopping bags in markets, butter tubs, flower bouquets, candy boxes, briefcases, and buses.

In addition to traditional explosives, jihadists are also attempting to educate themselves about chemical, biological, radiological, and nuclear (CBRN) weapons, which are incessantly discussed on jihadist forums. The "Encyclopedia of Poisons" offers a variety of methods to kill an enemy with a several toxic substances and is freely available to any member of the online jihadist community. Ricin and botulism bacilli are just two examples of individual poisons that have received much attention on jihadist forums. Members on these forums detail the speed with which a victim will die when receiving the poisons by injection, inhalation, or digestion. Other weapons of mass destruction, including nuclear and radiological devices have also been the subject of interest and instruction by the jihadists. One author, calling himself "Ozooo", produced a large compendium offering nuclear knowledge among other security, espionage, and military training.

In addition to physical preparation and military training manuals, the jihadists also impart knowledge to each about computer technology. Internet anonymity, of primary importance to members to avoid surveillance and capture, is frequently addressed. Al-Fajr Center, GIMF, and other jihadist media groups release cybersecurity manuals to aid the online jihadists. Al-Fajr Center created a specific cybersecurity magazine, "Technical Mujahid," which provides information remain anonymous online, how to utilize Pretty Good Privacy (PGP) software for encrypted communications, and detailed methods for a user to hide their sensitive files using a virtual machine. In its first pages, the "Technical Mujahid" states the jihadist stance concerning the virtual battle ground: "the internet provides a golden opportunity. . .for the mujahideen to break the siege placed upon them by the media of the crusaders and their followers in the Muslim countries, and to use [the internet] for [the sake

[7] Hamid Al-Ali. "Description of Martyrs in Paradise." Audio clip circulated on jihadist forums and posted on Hamid Al-Ali's official website at http://www.h-alali.info/snd_open.php?id=b75e9fb4–f2b5–1029–a701–0010dc91cf69

[8] http://www.alfirdaws.org

of] jihad and the victory of the faith." The GIMF provides similar information and recently distributed an encryption program built by the jihadists themselves to facilitate anonymous communications.

Tactical information is rapidly shared on jihadist messageboards. They study our analyses, distribute our reports, and quote our editorials, searching for our weaknesses. On their own initiative, jihadists are constantly providing data to the forums, posting maps of suggested targets, locations of American bases throughout the Middle East, and distributing aerial photographs captured by the Google Earth software, while others pull maps from government and university libraries.

Several primary jihadist websites house areas solely dedicated to training. Within these training areas, jihadists are encouraged to contribute their own expertise and data, so that all the jihadists can benefit from the knowledge of the entire jihadist community. Indeed, some of these forums even hold online training seminars, where less experienced jihadists can ask questions to jihadist weapons experts and receive direct responses online. In this manner, should any jihadist have difficulty in successfully manufacturing a bomb, or has a question regarding the procurement of required ingredients, there are thousands of other members, some with significant experience, who are available to provide the desired information.

By studying the training manuals and tactical material that exist on jihadist messageboards, warfighters can understand better the types of weapons likely to be used against them as well as the targets that jihadists are choosing for attack. Additionally, observing the training jihadists receive online will help security officials plan for threats discussed on jihadist websites, eliminating some of the guesswork involved in imagining the types of attacks jihadists are planning. While finding and destroying physical training camps will be essential to prevent jihadists from learning how to attack us, jihadists can instead rely on the internet for an interactive, comprehensive military education.

Online Communication and Coordination

Due to the efforts of security forces around the world, jihadists have an increasingly difficult time communicating and coordinating with one another utilizing traditional communication devices that can be easily traced, such as cellular or satellite phones. However, the internet provides a flexible, instant communication tools for jihadists. Whether via email, chat rooms, instant messaging services, e-groups, messageboards, websites, or voice over IP (VOIP), jihadists can communicate securely with one another rapidly using sophisticated, freely available encryption methods.

Jihadist media groups like GIMF and Al-Fajr Center release programs and training manuals to ensure that members of the online jihadist community know how to communicate with each other securely, using encryption methods like PGP. Groups and individuals desiring to form their own cells can therefore coordinate online with each other clandestinely below the radar of security officials. Even individuals spread across vast geographic areas can communicate with one another instantly and securely, forming virtual cells that work together. The members of these virtual cells may never meet each other in person but can nevertheless aid one another in planning attacks.

Established jihadist groups like al-Qa'ida can also communicate online to discuss everything from strategy to attacks. In one telling example, in December 2005, a top jihadist ideologue using the pseudonym Louis Attiyah Allah wrote to Abu Musab al-Zarqawi, discussing Zarqawi's role in Iraq and its place within the larger jihadist movement. At the end of the letter, Attiyah Allah notes to Zarqawi that he can be contacted on the "Ana Al-Muslim"[9] jihadist forum, indicating that even the top leadership of al-Qa'ida uses the internet to communicate.

As one notable example of cross-continental coordination, the infamous online jihadist Irhabi007, whose real name is Younis Tsouli, was arrested in England in October 2005 and was indicted under the UK's Terrorism Act 2000, with charges including "conspiracy to murder, conspiracy to cause an explosion, conspiracy to obtain money by deception, fundraising and possession of articles for terrorist purposes." Tsouli gained fame online for his teaching the global jihadist movement hacking and cybersecurity skills while facilitated the dissemination of jihadist propaganda coming from jihadist groups in Iraq and elsewhere.

As part of his online activities, Tsouli was also in communication with a jihadist cell in the United States. In March 2006, two Americans in Atlanta, Georgia, were arrested and eventually charged with "material support" to a terrorist group and are accused of plotting to attack oil refineries in the United States. These men, Ehsanul Islam Sadequee and Syed Haris Ahmed, visited Washington, DC, in spring

[9] http://www.muslm.net

2005 and recorded video footage of the U.S Capitol, the Masonic Temple, the World Bank, and a fuel depot. Remarkably, this footage was also found among Tsouli's belongings, indicating that the two American terror suspects were indeed in contact with Tsouli and were feeding him tactical information via the internet.

Aside from the obvious means by which small cells can coordinate and plan attacks through the internet, the online jihadist community has also engaged in coordinated cyberattacks on numerous websites. Because the jihadists can freely communicate while online, jihadists can designate electronic targets to a widespread audience and establish common timetables to launch cyberattacks. The electronic attacks usually involve "Denial of Service" (DoS) attacks whereby a targeted websites is flooded with requests at a single time. For these attacks to be successful, numerous individuals must attempt to access a website simultaneously.

Because the internet provides the jihadists a means to advertise the timing of a DoS attack to a large number of jihadists in a short time, these types of attacks only fail when too few jihadists participate in the attack at the same time. Prominent members of the jihadist Internet community, such as Irhabi007, have instructed jihadists in how to execute DoS attacks, and some groups that have announced a planned attack provide the necessary software with the address of the target already inputted. This method of attacking the enemy allows online jihadists to target Western interests from their own home and with little risk.

The results of these hacking initiatives have resulted in breaches of government security. Jihadists have hacked government and military websites and have retrieved extremely sensitive information on soldiers, including their areas of deployment, their health status, their social security numbers, their salary, their bank accounts, and other demographic information.

Jihadist cyberattacks launched on Dutch websites, including those belonging to the Dutch government, in January and February 2006 took many offline. The DoS operation, results, and images of a dead Theo van Gogh, a Dutch filmmaker who was murdered by a jihadist, were included in a video distributed shortly celebrating the attack. In another case, on November 27, 2006, a message was distributed on jihadist forums announcing the "Electronic Battle of Guantanamo," which was to target the websites of American stock exchanges and banks. The Department of Homeland Security warned about the attack and its danger, and though nothing came of the electronic jihadist operation, it fueled the desire for additional attacks. Even the Vatican's website was targeted by jihadists.

Retarding the ability of jihadists' to communicate is another necessary step in minimizing the jihadist threat. Though governments have done well in preventing jihadists from utilizing traditional means of communication, the internet remains the best communication device for the entire jihadist community. Allowing them to communicate instantly over vast distances, virtual cells can form quite easily, and coordinating cyberattacks requires a mere posting to a messageboard announcing the time and date of such attack.

While obviously we can never shut down the internet, we can monitor jihadists' use of the internet and track down their physical locations. Once jihadists learn that the internet is not a safe haven for their communications, many will become fearful of utilizing the internet as a means to communicate. It is unlikely that we will ever cut jihadist communication online to nothing, but at the very least, we can provide disincentives to jihadists using the internet by punishing those who do.

Strategy

The strategy behind the jihadist movement is not amorphous. Jihadist ideologues have developed a timeframe for their jihad, thinking both short-term and long-term, and understanding that success will only come after years of struggle. Major jihadist ideologues are able to direct the global jihadist movement by releasing white papers and books analyzing the situation of the jihadist movement and providing the jihadists with long-term strategies to ensure that the movement itself always has directions and goals. Jihadist strategies are released online and are widely circulated on jihadist forums so that the entire jihadist community can follow the same strategies and goals, reducing the discord amongst them.

One of al-Qa'ida's most important strategists subsequent to 9/11 is Abu Musab al-Suri, an al-Qa'ida operative who ran terrorist training camps in Afghanistan. Al-Suri's publications and studies are highly regarded by jihadists and are always housed on primary source jihadist websites and others. His 1600-page magnum opus, "The Global Islamic Call to Resistance," is an extremely influential jihadist manifesto and is available to download in a variety of digital formats. Jihadists discuss and analyze Al-Suri's writings both publicly and secretly to understand, develop, and expand upon his ideas.

In "The Global Islamic Call to Resistance," Abu Musab al-Suri details his theories of how to best wage jihad in the twenty-first century. The scope of the book is very broad, with topics ranging from a history of the Islamic world to autobiographical anecdotes about his role in the jihadist movement. However, a significant portion of the book discusses the most effective strategies for waging jihad against the West. Focusing on the types of attacks that will bring the mujahideen the most success, al-Suri advocates establishing self-starting, independent cells in Western countries with no direct affiliations to established jihadist groups. These cells operate to support the global jihadist movement, rather than any particular organization or leader.

Many of al-Suri's publications reiterate that jihadists must set up independent cells within their country of residence, bide their time, and only strike when the time is appropriate. Better, al-Suri intimates, to wait ten years studying and planning for a large, poignant attack rather than carry out a quick suicide bombing at a mall in America doing little damage. Al-Suri was arrested late 2005, yet, demonstrating the power of the internet, his strategies and theories continue to exist in cyberspace. Al-Suri's videotaped lectures at Al-Ghurabaa training camp in Afghanistan prior to 9/11 have been digitized and are available online as well. Whether dead or captured, the internet provides jihadists with a virtual immortality.

Available online, the publications of al-Suri and other ideologues share common themes in their strategies. These strategies include:

- Utilizing guerilla warfare
- Establishing self-starting, independent cells in Western countries with no direct affiliations to established jihadist groups
- Damaging the United States' economy through terrorist activities
- Attacking Arab governments that work closely with the West
- Attacking Western targets in Arab countries.

These strategies also include specific targets. For example, Al-Suri organizes the most important targets to attack in America and its allies as follows:

- Politicians
- Major economic targets, like the stock exchange, airports, bridges, metros, tourist attractions
- Military bases
- Media personalities
- Computers and information centers that connect the institutions of the country
- Jewish gatherings and notable Jews
- The offices of supranational targets, like NATO and the EU
- Buildings belonging to the CIA, FBI, and other security institutions
- Civilians, while avoiding women and children if possible, to prevent generating negative publicity

Obviously, these targets are not the only vulnerable individuals and institutions in the West. However, by studying and understanding the strategy the jihadist ideologues propose, we can better prepare ourselves against attacks that independent jihadist cells are likely to target. Also, we can develop more effective long-term counterstrategies against jihadists once we discern how they plan on expanding the jihadist movement. Therefore, the need to study jihadist strategies on the internet is paramount; it is an open window showing us how the jihadist movement will likely develop in the future.

Financing

Stemming the flow of money to jihadists is essential. Though carrying out terrorist attacks usually requires relative little money, jihadists do need funding for weapons, training, distributing propaganda, and the costs of hosting internet websites and messageboards. Since 9/11, the US, the UN, and other countries have worked hard to locate the methods and means by which terrorists transfer money. Prior to this crackdown, money was transferred to terrorist groups through sham front groups and charities or through offshore banking techniques. The US and others had much success in identifying the financiers of terrorism and exposing them.

While these traditional techniques no doubt still play a role in terrorist financing, jihadists have also turned to using the internet to transmit funds. Online remittance systems and other means of transferring money over the internet are constantly being used by jihadists to finance the jihadist movement. Jihadist webmasters use these electronic means to pay for their servers, and virtual jihadist groups have now appeared online soliciting donations from followers.

The Islamic Army of Iraq, an insurgent group operating within Iraq, released a video celebrating its October 15 attack on an American ammunition facility in Baghdad. Interestingly, this video ended with a plea for donations to be sent to "The

Electronic Nusra Society." Two days later, the group released the tenth issue of its online magazine, "Al-Forsan," which contained a full page advertisement seeking donations for the "The Digital Nusra Society." Though these advertisements offered no physical address to which to send donations, they indicated that donors could contact the group electronically for further instructions on how to donate.

Discussions on jihadist messageboards have gone into specific detail explaining how jihadists can donate online to jihadist groups. On the influential Al-Hesbah online forum, one jihadist described the process by which cash can be transferred through online remittance services. With certain online remittance services, individuals can add money to their online bank accounts by using cash to purchase physical cards (similar to phone cards) of various values from designated "brick and mortar" retailers across the world.

Using such an online bank account, an individual could then transfer cash to a jihadist group in the following manner:

1. The individual wishing to send jihadist groups cash purchases a physical bank card and transfers the value to an intermediary jihadist via an email with the required information to transfer the money.
2. The intermediary jihadist, in direct contact with the mujahideen, receives the online money transfer and then gives the mujahideen the value of the transfer in cash.
3. The jihadist groups receiving the cash from the intermediary can use the funds however they like, while the intermediary jihadist who received the initial online money transfer can use that money to purchase online goods.

As an example, a donor could purchase $100 worth of online virtual money from a physical store and then email the value of that money to an intermediary jihadist. That intermediary, now $100 richer, will give a jihadist group $100 in cash out of his own pocket. The intermediary, however, now has $100 worth of virtual money to spend online, while the jihadist group now has $100 in cash.

While this type of remittance is just developing and is only one way of transferring money, the chatter surrounding the ways to transfer money through the internet has been increasing on jihadist messageboards. Discovering and monitoring how jihadists transfer money online will enable us to further act against their financing methods, as we have done successfully before with traditional remittance services. If we are to continue our assault on terrorism financing, authorities must devise new ways to monitor and regulate online remittance services that can be abused by jihadists.

Conclusions

The internet remains one of the most valuable tools the jihadists have at their disposal, serving all the functions necessary to sustain a violent jihadist movement at minimal cost. Through virtual means, jihadists have in many ways replaced the training camps of the 1980s and 1990s that jihadist groups established in Afghanistan and elsewhere. Indoctrination, recruitment, financing, and training continue 24 hours a day on jihadist messageboards. A National Intelligence Estimate (NIE) Report produced in April 2006 and declassified in September 2006 agreed, "We judge that groups of all stripes will increasingly use the Internet to communicate, propagandize, recruit, train, and obtain logistical and financial support." [10]

In recent years, many have realized the extraordinary power that jihadists obtain by being able to exploit the internet. However, little seems to have been accomplished in preventing jihadists from using the internet to their advantage, directly harming our security, both domestic and foreign.

As long as the internet remains an uncontested safe haven for jihadists, the jihadist movement will continue to grow, regardless of the death or arrest of any jihadist leader or ideologue. The internet provides immortality to the ideology behind the jihadist movement, and countless individuals can absorb this propaganda, which is readily available in numerous languages. While not all individuals exposed to jihadist propaganda will succumb to it, the images, sounds, and thoughts that the jihadists produce are carefully woven, attractive, and compelling. Many will buy into the ideology and become part of the online jihadist community. So long as this virtual community exists unopposed, jihadist groups will always be able to refill their ranks and keep their movement alive, indoctrinating and training their future army.

The challenge now is to infiltrate and erode this virtual network to weaken this driving force behind the global jihadist movement. Studying the online jihadist community empowers us. We can listen to what they say, understand the way they think, and determine how they operate. We can grasp their ideology and devise ef-

[10] http://odni.gov/press__releases/Declassified__NIE__Key__Judgments.pdf

fective counter-propaganda. We can better defend known targets, identify potential threats, devise countermeasures to their tactics, undermine their strengths, and exploit their weaknesses. There is a wealth of information available online, if we are willing to take the time to collect, study, and analyze the data.

To take advantage of this online intelligence and counter the jihadists on the internet, policy makers and authorities should embark on the following steps:

1. Understand how jihadists utilize the internet, including the hierarchy and structure of online jihadist networks, the technical process of distributing the videos, and how jihadists exploit services on the internet.
2. Effectively monitor jihadist activity on the internet. Because monitoring the entire internet is impossible, understanding the hierarchy of online jihadist networks will help focus efforts on the most important websites and other internet services the jihadists use.
3. Identify and exploit the weaknesses of the jihadists on the internet.
4. Mine jihadist activity on the internet for intelligence. By successfully infiltrating the most important jihadist forums, more specific, actionable intelligence can be obtained than simply by monitoring secondary and tertiary jihadist websites. This intelligence can then be used to deal severe blows to the global jihadist movement.

For as long as jihadists on the internet can engage in terrorist activities unfettered and unmonitored, the U.S. will not be able to cause significant, lasting damage to the global jihadist movement. The internet plays a key role in fostering homegrown radicals, providing them with all the information necessary to conduct local attacks as well as a location to meet and plan without being detected easily. If the global jihadist threat, both domestic and abroad, is to be combated effectively, the U.S. must invest significant resources into studying, monitoring, and understanding how jihadists utilize and exploit the internet.

Ms. HARMAN. Thank you very much for that fascinating testimony and for the video that we will see in a few minutes.

I now recognize Ms. Aftab to summarize her statement for 5 minutes.

STATEMENT OF PARRY AFTAB, INTERNET ATTORNEY

Ms. AFTAB. Thank you, Madam Chairwoman. You have to forgive me, I have laryngitis, which is perhaps a good thing for a lawyer to get.

Madam Chairwoman, Chairman Thompson, ranking member and other honored members of the committee, thank you very much for inviting me to speak here today. In addition to the credentials outlined by Chairwoman Harman, I am the executive director and founder of WiredSafety.org. We are the world's largest Internet safety and help group. I have 13,000 volunteers in 76 countries around the world, and we deal with all aspects of Internet privacy, crime and security, especially in connection with children.

What I have to offer today is very interesting because it is totally different from everyone else on the panel. I will be talking about how the radical groups and homegrown terrorism groups can spot vulnerable children and young adults.

We teach our children to be careful about the information they share online. They are now all using MySpace, Facebook, Bebo, Pixo, Tagged, innumerable sites like YouTube where they are sharing personal information and supplying it to others. The same way that they are beating each other up in hallways and putting those things on YouTube, we have groups that are trying to make themselves look glamorous and to recruit young people who are looking for glamour.

Many of our young people are looking for their 15 megabytes of fame. They want other people to look at their video, what they have to say. They want to have thousands of friends on MySpace.

They want people to rank them as a site to go to. They want to be seen as influencers. They are looking for someone to listen. In doing this, they are able to broadcast their vulnerabilities. They are easy pickings for the groups that are looking for radical members, and they are recruited at different levels. Either they are recruited as manipulated innocents, people who have no idea that they are being manipulated but are promoting sites and ideologies, ranking videos and sending links across the Internet. There are supporters that are sort of interested but not really sure why, who will bring up the profile in the rankings on MySpace or YouTube by hitting it, ranking it, commenting on it in a productive way that will bring more traffic. There are influencers. A lot of influencers on the Internet have a site that people watch. They are the people they turn to. They may not be the people they turn to in real life, but for whatever reason, they have the panache online that will attract others. If the radical groups can reach one of these influencers, even if the influencer doesn't buy in, isn't a member, they can influence millions upon millions of others who will go where they tell them to go online.

There are sympathetic users, people who comment about how they are angry with the United States. A member of their family may have been in the Armed Forces and hurt. They are frustrated with politics, and they show themselves as potentially sympathetic recruits.

There are vulnerable ones who may have been targeted and bullied. They may have felt threatened, and they are looking for a safe place.

There are target group members, members of a religious or an ethnic group that are the targets for recruiting for these organizations. And all of these things are being put on profiles, millions and millions of them, online.

And there are seekers. We have always found that the issue with young people and dangers online is a direct product of boredom versus unsupervised time plus bandwidth. So if they have a lot of connection and they are all connected on their cell phones, interactive gaming devices, and on the Internet through Web 2.0 technologies to broadcast their beliefs and talk to each other, they are there.

What do we need to do? We need to make sure that the Internet industry, the social networks in particular, are working closely with the committee. The commissioners should put it together. WiredSafety has worked within them for many years and is responsible for privacy settings on MySpace and other sites.

We are creating a new center called Wired Trust that not only will advise the industry how to find dangerous content and people and movements on their networks, but to police them, to report them to law enforcement and to organizations that need to do something about it. And if they don't know how to do it, we will do it for them. That will launch in the spring to make it easier. We will train them how to do it, give them technologies to make it easier and spot high traffic sites where you know there is something going on, whether it is child predators, sexual content or radical groups. Because they really are no different. We need to make sure that teachers and others understand the difference between

truth and misinformation and hype, whether it is MartinLutherKing.org as really a hate site, or saying that the Holocaust never happened, or any of the other sites that make radicalization look like a score and will attract young people who are bored with technology and money in upper-middle-class neighborhoods, kids who never would have been exposed to this otherwise, who are not Muslims, who are not normally interested in radical groups, who see it as a way to become included, a way to become famous, a way to become in, a way to find a place to belong. And for that, WiredSafety and all of my 13,000 volunteers and myself offer any of our expertise and experience with dealing with this for 12 years now to this committee and subcommittee and the New York Commission, should you need that.

[The statement of Ms. Aftab follows:]

PREPARED STATEMENT OF PARRY AFTAB, ESQ.

SUMMARY

Our children and young adults are online. They do their school work, entertain themselves, communicate with each other and us, research things, shop for things, learn and work, and compare prices online. They need the Internet for their education, their careers and for their future. Of all the risks our children face online, only one is certain. If we deny our children access to these technologies, we have guaranteed that they are hurt. All other risks are avoidable through a combination of awareness, supervision, trained law enforcement investigators and the adoption of best practices and risk management by educational institutions and the Internet industry itself.

This testimony will focus on the darker side of the Internet, especially Web 2.0 technologies and social networks. I respectfully caution this Subcommittee not to consider throwing the Internet out with the cyberrisks bathwater. As I have said over and over for the last twelve years, all risks can be contained and managed with the right combination of analysis of the risks, measurement of their impact and evaluation of use of the technologies.

This requires that we engage the Internet industry itself and advise them in ways to build safer technologies and adopt best practices designed to make all their users, not just children, safer. It also requires that we engage law enforcement agencies in discussions with the industry and cybercrime prevention non-profits, such as WiredSafety.org, in forming and deploying solutions.

OPENING STATEMENT

Good afternoon, Chairwoman Harman and other esteemed members of this Sub-Committee. I would like to thank this Sub-Committee for inviting me to testify today and share my expertise on young people online. I will focus my testimony today on how radicalization and homegrown terrorism groups can use the Internet to reach at-risk youth and recruit followers from the ranks of teens and young adults. I will also suggest ways we can address these risks, in particular ways Congress can help address them.

My name is Parry Aftab, and I am an Internet privacy and security lawyer and founded and run the world's largest cybersafety and help group, WiredSafety.org. I have worked in the field of cyber-risk management and cybercrime prevention since the Web was launched in 1993. I was appointed by UNESCO to head up its online child protection initiative in the United States and formed and run a charity that contains more than 12,000 volunteers from around the world. WiredSafety.org's special group of trained volunteers offer one-to-one help to victims of cyberabuse and assist law enforcement, parents, schools and communities manage online risks and prevent cybercrimes. We see all risks, on all digital technologies for all ages of users on a daily basis.

My testimony will pull from my personal experience, that of the charity, our work with law enforcement and regulatory agencies and extensive polls of young people. It will focus on how Web 2.0 technologies and networks are allowing radical groups access to young users and the ability to spot more vulnerable and at risk youth for recruitment.

Identifying the Problem

Most of the teens and young adults in the United States are using social networks and other Web 2.0 technologies. These include MySpace, Facebook, Bebo, Xanga,

Google's Blogspot and its new social network—Orkut, BlackPlanet and MiGente and Hi5, as well as X-Box 360, PSP2, DS, World of Warcraft, Runescape and other interactive gaming sites and technologies. It has fast become their favorite online activity, after instant messaging.

While accurate statistics of minors' use of social networks do not exist (with many lying about their age or identities), statistics as to social network traffic and usage of all registered users are regularly tracked.. According to HitWise, a leading industry reporter, MySpace traffic accounted for almost 5% of all US cybertraffic, with Facebook accounting for almost 1% of all cybertraffic during the week of October 13, 2007. And all social networks in the US combined accounted for almost 7% of all online traffic during the same time, up about 20% from last year.

They use it to communicate with others, either existing friends in the real world or new ones in the virtual world. They use it to share ideas and showcase their talents and interests. They use it to persuade others to take action on important issues. They use it to network with others and recruit people to their cause or candidate. They use it to find other like-minded people or people who are different from them. They seek out what others are doing in big cities, affluent communities, other countries or next door. They look for love and romance and excitement. They search for long-lost friends, kids they went to camp with and former classmates. They post pictures and video, using their computers, cellphones and iPods. They share secrets and vulnerabilities, looking for someone to listen. They exploit the secrets and vulnerabilities of others. They lie and steal, learn and teach. They promote content, people and causes by tagging and commenting and rating profiles and multi-media content. And they pose as someone else, or something else to try on new personas or lifesyles. They influence and are influenced on these networks. They do it for the same reasons young people have always done things. They do it for good, for bad, for fun and for kicks.

While most of the media and governmental investigations have focused on the more traditional risks of pornography, Internet sexual exploitation, cyberbullying and harassment online, other less obvious risks have been largely ignored. These include gangs and hate groups, suicide threats, serious eating disorders, scams and fraud, violence, misinformation and hype, commercial espionage and warfare and, now, radicalization.

For the same reasons other users are setting up profiles and posting videos online, gangs, radical groups and even terrorism groups are harnessing the power of the technology and Web 2.0 to spread their messages, communicate with others and recruit others ot their cause. While that is expected, the surprise comes when we see our young adults and teens being receptive to these tactics.

We are seeing an increase in upper-middle class high school students joining inner-city gangs, seeing them as exciting and fun. Many young people are searching for leadership or a cause to believe in. They are seeking a place where they are accepted and can belong. And never before have they had as many to choose from, all at the click of their mouse, or from their cellphone or gaming device. And because they often do things online that they would never dream of doing in real life, they tend to engage in riskier behavior online and often don't see the line between observing and joining, between curiosity and recruitment. Perceived dangers are seen as exciting. And behind their computers, in the privacy of their home, they give the predators the information they need to push their buttons. They signal their vulnerabilities and what they need and are seeking. They make it easy. Too easy for those who are looking for vulnerabilities. Too easy for radical groups and homegrown terrorism groups.

Young People on Social Networks and Using Web 2.0 Technologies

Social networking, a combination of mini-webpages, blogs and searchable communities, have expanded in recent years, most recently exploding with the growth of MySpace and Facebook. Based upon our polls, we estimate that more than half of the young teens in the US with home Internet access have at least one social networking profile and more than 80% of university students have at least one social networking profile.

Many have 2 to 5 separate profiles on just one site, and most have at least one profile on two or more social networks (not all being used, however). Most users check their profiles and their online networks at least once a week, and in many cases several times a day.

WiredSafety.org and I first began our social networking safety work in 2004, after learning how many young teens and preteens were beginning to use them. Unlike the early AOL profile pages used by teens and preteens in prior years, where the young users could post their contact information and brief statements about their interests, these networks were designed to be interactive. And instead of dry posts

of contact and other personal interest information, these networks allowed users to post music, movies, animations, sounds, images and lots of user generated content to their page. When used effectively, this allowed the sharing of ideas and expertise and communication with real life friends. When misused, this allowed the broadcast of vulnerabilities that predators of all types can exploit to target young people. This is when the real dangers arise.

While the media and many others have focused only on the dangers of these networks when used by preteens and teens, it is important that we keep our eye on their good uses and value and why their use has exploded in the three years. We have spent four years studying how and why preteens, teens and young adults use these kinds of sites.

Most use them for innocent purposes. They want to find their friends and communicate among larger groups than they can do via instant messaging. They can post something and know everyone in their class or group can read it at the same time. They want to show off their creativity and how special they are. And they can pretend to be prettier, more popular, richer and more famous than they are in real life. They raise money for their favorite charity and awareness for new causes.

They can post one message and their 150 best friends can see it right away. Unfortunately, so can those who might not have their best interests at heart. And sadly, in some cases, our teens are acting out, taking risks and exploring involvement with hate groups, gangs and radical groups that promote violence. That's when things can get dangerous, especially for young teens.

Professional Guidance for the Industry and Adoption of Best Practices

Most members of the Web 2.0 industry have set rules for what can and cannot be done on their sites. These are set out in their "terms of service" or "codes of conduct." Most terms of service already forbid radicalization (using language about "promotion of violence"). But forbidding it and spotting it are very different. They typically rely on reports of terms of service violations ("TOS violations") to enforce their rules. They sometime deploy technology and live moderation staff to police their site, independent of the reports.

For example, MySpace set up an image scanning procedure, looking at hundreds of thousands of images each day for sexual content and gang signals and hate images. The majority of their policing, however, occurs when a user reports another for a TOS violation. This is then handled under their existing procedures for that category of violation. They are also, according to reports, scanning their system for registered sex offenders.

This is unusual, though, and limited. Only a small protion of images posted can be scanned. The traffic is too large for existing moderation teams to police effectively. Most networks rely entirely on user reports, since video and other multimedia are difficult to filter and review for contraband content.

Social networks, starting with MySpace in early 2005, have come to me and to WiredSafety for help in managing risks and creating safer experiences for their users. They have sought our help in designing law enforcement investigator's guides to assist law enforcement when evidence of cybercrimes needs to be obtained from those sites. But their needs are greater than what a cybersafety charity can provide. They need hands-on training, certifications of practices and technologies, enhanced technologies and security practices, guidance on adoption of best practices and ways to avoid cyber-abusive and criminal behaviors. They need to share effective practices with each other in industry leadership councils. They need to anonymously share vulnerabilities they have identified to make the industry itself safer, without losing competitive advantage. They need to train recruit or outsource monitoring and moderation staff, and do it in multiple languages.

Because of our unique experience and over 12 years in this field and because managing risks online in a Web 2.0 environment is like "herding cats" the networks and industry has requested that we deploy our experience in helping create best practice standards and assist in their implementation. In response to this demand, leaders in cybercrime and cyber-risk management and security have joined together to form a center for the Web 2.0 industry that will train the industry, advise the industry and provide tools and expertise to implement best practices, and in certain cases, handle moderation and site policing for these sites. The center will be called "The Wired Trust" and will work with the charity, but be a commercial entity designed to serve the needs of the Web 2.0 industry and those involved in funding advising the industry. Among other risks, The Wired Trust will help manage risks of radical groups and terrorism groups using these networks to recruit and promote their violent missions.

Leaders in the industry are already lining up to join The Wired Trust and find ways to become safer and prevent risks.

It's a start.

Public Policy Solutions, Approaches and Congress's Role

The solution is not blocking or limiting access to Web 2.0 technologies or social networks. Creating a new law prohibiting schools and libraries from allowing underage students and users to access these sites or otherwise locking young people out of these sites seems an obvious approach. While this may appear on its face to be an easy answer, it is neither easy nor the answer.

As more social networks are launched every day, and every ISP, entertainment company and wireless provider is either building a social network or finding a way to integrate social networking and community interactivity into their new and existing sites, it is impossible to block all of them and not other valuable Internet features, sites and content. Instead, schools need to be armed with the tools and risk management expertise to decide what sites their students can access during school hours from their servers and how to enforce their decisions and policies.

Schools need to decide if their students should have access to any non-educational site from school computers, and if so, which ones and for what purpose. They then need to develop a policy communicating this decision and the rules to the students (in language they understand), the teachers, the parents and other caregivers and to their IT team. They need to decide whether they will be using software to help enforce their policy, or merely traditional discipline for violating school policies. That too needs to be communicated to the school community. They also need to create or adopt educational programs teaching their students what information they can and shouldn't be sharing online, the risks of irresponsible Internet use and where to go when things go wrong.

Teaching students about hype and misinformation and about hate and radicalization is crucial as well. If young people learn how they are manipulated by these groups, they are less likely to fall prey to them. At risk youth needs to be supervised, as they are often the earliest targets and most likely to join radical groups that promise them excitement and community combined. Educational institutions can play an important role in teaching their students, parents and other community members about safe, private and responsible Internet and wireless technologies use. This spans all risks, including radicalization.

For this to happen effectively, we need better research. We need reliable information and studies on which educators and others in risk management can base their decisions. They need to be apprised of new trends and developing risks. They need to know that websites and services are using the latest and best technologies and have adopted the best industry practices with their users' safety in mind. They need help that Congress can provide by getting behind these research initiatives.

Congress can also be very helpful in helping gather relevant information about cybercrimes and abuses. I have testified previously that actual cybercrime statistics are lacking. Everything we know is largely anecdotal. In 1999, the FBI's Innocent Images (charged with investigating crimes against children online) opened 1500 new cases of suspects who were attempting to lure a child into an offline meeting for the purposes of sex. Based upon my estimates, about the same number of cases were opened by state and local law enforcement agencies that year. The same year, approximately 25 million minors used the Internet in the U.S., Now, with more than 75 million young Internet users in the U.S. we don't know if the number of instances have increased, decreased or remain flat, given the growth. The crime reporting forms don't collect information about the use of the Internet is child sexual exploitation crimes, or any other crimes. That has to change.

Creating a central reporting database where all instances of cybercrimes are reported for statistical purposes, from radicalization sites and networks, to cyberharassment to Internet-related ID theft, fraud and scams, to sexual predators and Internet-related child pornography and sexual exploitation would be incredibly helpful. It could track cybercrime trends affecting adults, seniors and youth. It could be used to help design safer systems and best practices and guide legislation directed at a meaningful problem, in a meaningful way. This is the kind of centralized reportline that could be managed by the FTC or other governmental agencies.

In addition, with tax dollars becoming more and more precious and the mission of all Congressional representatives to put tax dollars into the most effective use, existing programs by trusted non-profit groups can be highlighted and made available online to schools and community organizations that need them, without cost. Without having to reinvent the wheel, massive amounts of programs, lesson plans and risks management guides already exist that can be used as is, or easily retooled. Finding a way to get these wonderful resources into the hands of those who need them the most, using interactive technologies and the Internet and mobilizing volunteers to help deploy existing programs that were developed with or without

government dollars. Focusing attention on what works and what doesn't is something that Congress does best. WiredSafety.org and I pledge our help in doing that. It's time. And hopefully, not too late.

Ms. HARMAN. Thank you very much. And thank you for coming in spite of your laryngitis.

Mr. Weitzman, you are recognized for 5 minutes. And let me inform witnesses and members that we are expecting four votes very soon. We will get through the testimony; and then, if the votes are called, then we will recess as briefly as possible for those votes and come back. I hope that won't inconvenience the panel.

Mr. Weitzman, please summarize your testimony for 5 minutes.

STATEMENT OF MARK WEITZMAN, DIRECTOR, TASK FORCE AGAINST HATE, SIMON WIESENTHAL CENTER

Mr. WEITZMAN. Thank you, Madam Chair and members of the committee, for inviting me to speak to you today on such an important topic.

Let me begin by saying that we have been tracking, the Simon Weisenthal Center, instances of Internet extremism going back to the mid-1980s when they began as offshoots of U.S. extremists, such as Tom Metzger, Louis Beam, David Duke, et cetera, in the early bulletin board systems that have subsequently expanded.

One of the things that we have discovered is that some of the methods used by both our homegrown extremists as well as international extremists are the same. By trying to appeal to a closed group, that is create a closed environment, they help influence the process of radicalization as has been described earlier.

I am not going to continue by summing up the written testimony as much as I would like to demonstrate some of the things that we are talking about and the panel has discussed already. So we have a short PowerPoint that I would like to bring into this as well and illustrate some of the things that we have talked about.

Some of these are conspiracy theories that present a closed view of the world, such as blaming 9/11 as part of an outside job or a job by outside groups, such as the U.S. Government or Jews, et cetera. Some of these are pro-Iraqi insurgency videos. Some of them are media portals that people can enter into. The ones that you saw earlier with the flags on them, the U.S. flags, show that they were based on U.S. servers.

These, as we keep going through, we can see that these are again from al-Qa'ida, but you see the cross of Christianity, the Star of David, et cetera, as the symbols being under attack.

And this is just a chart that shows how to attack and break up the U.S. Forces in Iraq. And if we keep going through there, we will see that, as a matter of fact, the CIA is even mentioned by name in it. That is followed by a Taliban document Web site, a Taliban chart that deals with how to—

Ms. HARMAN. While you are doing this, these are readily accessible to our teenagers and young adults?

Mr. WEITZMAN. These are readily accessible. There is actually nothing to stop them.

I apologize for the delay. The al-Qa'ida principle of jihad, what they talked about electronic jihad and talked about literally tracking American and Jewish and secular targets as well.

There is an encyclopedia of jihad available online, showing here how to make a car bomb, and it continues as we go through, cyanide bombs. You can see for yourself all the way through, how to use cell phones as detonators. And this again, translated to English, Rules of using or making explosives and how to be careful around the explosives, and so on.

There is a Taliban training manual that I mentioned earlier. And you can see again cell phones and other items, including RPG, rocket-propelled grenade launchers.

And if we keep going through, we will see, again, GPS systems being used.

So these are really manuals of how to become a jihadist online. The Media Sort Campaign is online, I just went into it last night and found items that told you exactly how to train to enter a non-Islamist music forum, for example, and to use that as a propaganda tool for getting your message across. Discussion groups based in the United States as well that bring these topics into anyone's home.

And, finally, these are some Latin American sites that use Iranian propaganda word for word and also linked to U.S. extremist sites; for example, a U.S. site that talks about exiling—has a poll to exile blacks from every Western country and claims 100,000 people have voted in favor of exiling blacks. That would be the that site.

And if we keep going through, coming to the next category are the category of online games which are used to attract children. Some of these games, for example, the game of New York Defender, which was originally Russian in origin. Then this is an anti-gay game, where you have to kill the gay guy before rape. Or, how to be a suicide bomber. Finally, the Border Patrol. The object is to shoot as many illegal immigrants coming across. Now, obviously, the game is targeted to young people, help to inculcate a mindset in them, and to change that into a social policy, such as supporting stringent controls.

And then, finally, we end with a site that literally talks about the bombing of, "soon, soon, soon will be the attack on Manhattan, dated September 2, 2007."

So, I mean, I think, as I said, in some ways, the best way to have illustrated the problem along with the written testimony was these sites.

In conclusion, if I could just mention a few very brief recommendations. First is that we have to be aware of the empowering effect of the Internet on extremists. We must have researchers and responders who have both the technical and linguistic skills to keep us informed and to be able to respond to what is online. We must make users aware of the misinformation and the techniques used by extremists. We must have increased cooperation internationally among the political, law enforcement, NGO, academic and all other interested sectors. There must be the political will to legally act when necessary.

We also must be prepared to invest in positive sites—so far, we have talked only about negative—but in positive sites that can present alternative narratives to that that is being constructed by the Islamists. We at the Weisenthal Center have made a start in

that by creating a site called AskMusa.org, which is an attempt to present, in Arabic, Farsi, and other languages, views on Jews and Judaism not related to the Middle East conflict and directed in a mediated fashion.

In many ways, we have ceded the Internet to our enemies, and the result has been extremely harmful. However, even in a globalized world, there is no reason to believe this condition is permanent. But we need to focus our efforts better and to invest more resources in the struggle. As the famous Holocaust survivor, the namesake of our Center, Simon Weisenthal, wrote in 1989, "The combination of hatred and technology is the greatest threat facing mankind. How we face that threat might well define the world we live in the near future." Thank you.

[The statement of Mr. Weitzman follows:]

PREPARED STATEMENT OF MARK WEITZMAN

Good Afternoon. Thank you, Mr. Chairman and Members of the Committee, for inviting me to speak to you today on the topic of "Using the Web as a Weapon: the Internet as a Tool for Violent Radicalization and Homegrown Terrorism." My name is Mark Weitzman, and I am the Director of the Task Force Against Hate and Terrorism for the Simon Wiesenthal Center. I am also the Simon Wiesenthal Center's chief representative to the United Nations.

While I often begin my presentations by saying that we at the Simon Wiesenthal Center have been tracking extremism online since 1995, the reality is that we actually began much earlier. By 1983 and 1984, various domestic extremists such as George Dietz, Tom Metzger and Louis Beam were already using the Bulletin Board Systems to post material for their followers and others.[1] The potential that these earliest users saw was later realized, leading one United States white supremacist to declare a decade later that "the Internet is our sword."[2]

Some, like David Duke, saw the Internet as not only being a revolutionary communications medium, but as having great import for their own revolutionary ideas. For example, Duke wrote on his website, "I believe that the Internet will begin a chain reaction of racial enlightenment that will shake the world by the speed of its intellectual conquest."[3] Duke's longtime friend, Don Black, together with Duke's ex-wife(and Black's future wife), Chloe Hardin teamed up to begin Stormfront on March 27, 1995, which is generally credited as being the first extremist website, and which today is still one of the most prominent and important sites online.[4]

The Oklahoma City bombing brought domestic extremism into sharper focus, and the increasing use by the general public of the Internet quickly led more domestic extremists into the electronic age. At that time we began to publicly track that growth, and have continued to do so. The growth has been explosive, with our database growing from 1 (Stormfront) at the time of the bombing of the Alfred Murrah building on April 19, 1995, to over 7,000 today. Initially, the overwhelming number of those sites came from what could be described as Western extremists. These included skinhead, neo-Nazi, white power, ethnic and religious extremist, homophobic and conspiratorial sites, and the numbers showed steady growth, as did the technical capabilities of the sites. They were used to recruit, to raise money, to propagandize, to incite, and to provide a virtual community to hitherto far-flung fellow believers. By doing so, the Internet came to be viewed as empowering a whole new generation of extremists.

The next defining moment was 9/11. The attacks on the United States signified a new stage in Internet extremism, with Islamist extremism rapidly exploding online. I use the term Islamist in contrast to Islam to signify the radical jihadist and extremist ideology. At the time of the attacks, there were almost no such sites. Today, they number in the thousands.

---

[1] http://www.publiceye.org/hate/earlybbs.html. Kenneth Stern, *A Force Upon the Plain,* Simon and Schuster, 1996, p. 226.

[2] See my article "The Internet is Our Sword: Aspects of Online Anti-Semitism," in John Roth and Elisabeth Maxwell, Eds. *Remembering for the Future: The Holocaust in an Age of Genocide,* Vol. I, pp. 911–925, Palgrave, 2001.

[3] *Ibid.*

[4] http://www.stormfront.org/dblack/racist__021998.htm.

As might be expected, in some ways the use of the Internet by Islamist extremists resembled the early stages of Western extremist use, as they both began at a relatively simple level before moving on to more complex usage. However, from the very beginning, the Islamists who planned 9/11 were more sophisticated in their approach, using the Internet for planning and communication. Of course, part of that can be attributed to having the benefit of the growing technical capabilities of the Internet, as well as reflecting the growth in cyberknowledge of its users.

The reasons for this phenomenal growth are varied. The Internet is, as an early observer wrote "subversive, because [it] offer[s] potential enfranchisement to the disenfranchised and voice to the voiceless."[5] It allows individuals who are isolated or alienated, both physically and psychologically, to feel that they are linked, empowered and members of an international movement. For some young Muslims in the West, who are living in an environment where they are alienated both from the majority culture and from the traditional structures of Muslim life that have broken down in the West, the Internet provides access to a radical form of Islam that gives seekers the virtual environment that they are searching for. This is seen as a purer and uncompromised version of the religion, and thus strengthens its appeal by creating a strong demarcation between the moderate version and its more extreme manifestation.

Radicalization can be a result of this relationship. The Internet, and its idealized and radicalized virtual community, overtakes the perceived dismal reality of the real world, and provides an authoritative narrative that creates its own reality. This reality is constructed to fill a void, and its prime target is youth, especially those alienated in some way from their surroundings. The use of professional, slick and appealing sites, videos, chat rooms, newsgroups, etc., are all forms of communication that are commonly used by younger users who are prepared to take the information they receive at face value.

This points out another important aspect of the Internet. As Ian Buruma has written, "The Internet. . .lacks a superego that filters out the monster from the depths."[6] This means that there is no editorial control, and anyone can present himself or herself as the expert, or the authoritative face of a religion. In this case, because of the social and psychological factors described above, Islam is presented as a pure and moral religion under continuous assault from the corrupt, immoral West, especially embodied by Israel and the United States. This narrative is illustrated online by references and visuals from areas of conflict, all carefully edited to fit into various aspects of the narrative (Islam as victim, Islam victorious, etc.).

This trend was summarized by an Arab Human Rights website that wrote, "Starting from a few years ago, observers have noticed a growing religious trend in Arabic web pages: The majority of Arabic language web pages are either about Islam, as interpreted by those responsible for the websites, or are calling for the spread of Islam. . . ." The majority of Islamic web pages all call for the adoption of the extremist Sunni interpretation that has spread widely in the Arab Gulf area and extended to reach other Arab states, non-Arab Islamic states like Afghanistan and Pakistan, as well as Muslims living in Europe and North America. . . . In spite of the fact that many of these Islamic web pages preach religious hatred against non-Muslims and even against other Islamic groups, they have managed to slip past the bans and the filters put in place by Arab states. Many Arab governments practice selective censorship; that they permit the continued existence of these Islamic sites is less a result of a respect for the freedom of expression than it is a reflection of their satisfaction with the content of these websites."[7]

In many ways the Internet favors the religious extremist. It allows anyone to set himself or herself up as an authority figure, to the extent that reports last year indicate that some lesser-known Muslim leaders had overtaken Osama bin Laden as the leading figure in the jihadist movement.[8] They did this by using the chat rooms and online forums to establish their authority, and while some might react by saying that anything that cuts into the influence of bin Laden is good, the reality is that this means that even the removal of bin Laden or Ayman al-Zawahri would have no impact in threatening the movement. And, since one of the effects of this online communication is that the more radical posters are the ones to stand out, and so

---

[5] Matthew Friedman, Fuzzy Logic: Dispatches From the Information Revolution, Montreal, Vehicule Press, 1998, pp. 82–83, cited in Weitzman, above.

[6] Buruma, "China in Cyberspace," New York Review of Books, Nov. 4, 1999, p. 9, cited in Weitzman above.

[7] "The Internet in the Arab World: A New Space of Repression?" The Arabic Network for Human Rights Information, http://www.hrinfo.net/en/reports/net2004/all.shtml#14. The report claims that there was a decrease in these sites after 9/11, an assertion that seems to be at odds with all other researchers' findings.

[8] "Qa'ida Leaders Losing Sway Over Militants, Study Finds," New York Times, Nov. 15, 2006.

the discourse is often ratcheted up, with the result being an even more militant or radicalized leadership and followers.

The growing sophistication of the Islamists is also apparent in the production values of their sites. Whether it is in the use of different media, such as videos and games, or different languages, the Islamist outreach is much more attractive and accessible. Part of this can be attributed to Arabic sites and organizations that have recognized the need to reach a large audience, but part of it is also the result of Western Muslim extremists, some of whom are converts, who have taken the familiarity they have acquired by living in the electronic society as well as taken advantage of the rights granted to them by those societies, to create and post Islamist and jihadist websites. By literally speaking the language of their targets, they represent a significant growing factor in online Islamist extremism.[9]

To illustrate the trends described above, we have put together a short PowerPoint demonstration. Without going into deep detail in these written remarks, I would like to offer some brief descriptions of the material that will be shown. The presentation begins with a look at how 9/11 is viewed in some eyes online, including those who applauded it as well as some conspiracies sites. The presence of the conspiracy site is significant, since so much of what passes as fact online is actually based on some form of conspiracy. These are often built around the Protocols of the Elders of Zion, which allege Jewish control of the world, or around presenting the United States government as being engaged in various conspiracies or cover-ups, or ultimately having the entire Western world engaged in a vast, multi-layered conspiracy against the Islamic world.[10]

Next is a series of sites of media portals which show some of the varied methods that the Islamists use to get their message out, including some based on United States servers. These are followed by some looks at charts and other manuals on how to use violence, along with a novel interpretation of jihad that calls for an "electronic jihad."

There are jihad discussion groups and some Islamist sites aimed at Latin America (a new target), as well as some links to extremist right-wing groups like Neo-Nazi, etc. It is worth pointing out that some observers have noted the attempts online to bring Islamist and right-wing extremist groups together, which are often visible in cyberspace.[11]

Next are a series of games that show some of the different themes used by all sorts of extremists, and how they target youth by tapping into fears and issues that the extremists attempt to manipulate. Finally, I end with a look at how the United States is still specifically threatened.

Conclusions

The Internet has become as real a battlefield as exists anyplace. It provides a haven and an opportunity for Islamist extremists to recruit, educate, communicate and bond in a secure, protected environment. As a result, in many ways it is the prime factor in the radicalization of many of recruits to the jihadi ideology. This factor calls for increased attention and efforts to counter the growing influence of the Internet in these areas. Some steps that might aid in this effort include:[12]

(1) We must be aware of the empowering effect of the Internet on extremists.
(2) We must have researchers and responders who have both the technical and linguistic skills to keep us informed, and to be able to respond to what is online.
(3) We must make users aware of the misinformation and techniques used by extremists.
(4) We must have increased cooperation internationally, and among the political, law enforcement, NGO, academic, and all other interested sectors.
(5) There must be the political will to legally act when necessary.
(6) We must be prepared to invest in positive sites that can present alternative narratives that might counteract the Islamists material (i.e., the Simon Wiesenthal Center's new AskMusa.com site that presents Jews and Judaism in four major Islamic languages directly to the Muslim public).

---

[9] Home grown Web site funnels Islam's extremist views to world, New York Times, Oct. 15, 2007.

[10] On the Protocols, see Steven L Jacobs and Mark Weitzman, Dismantling the Big Lie, Ktav, Hoboken, 2003, pp. 1–7.

[11] See George Michael, *The Enemy of My Enemy: The Alarming Convergence of Militant Islam and the Extreme Right,* University of Kansas Press, 2006, as well as my forthcoming article, "The Globalization of Anti-Semitism and Holocaust Denial," which is scheduled to appear in the volume, Lying About the Holocaust, edited by Robert Wistrich.

[12] Most of the following proposals were presented in my remarks to the OSCE Expert Meeting on Best Practices in Combating Anti-Semitism, Berlin, Nov. 20–21, 2006, which can be found in the Conference Documentation, p. 92.

In many ways we have ceded the Internet to our enemies, and the result has been extremely harmful. However, even in a globalized world, there is no reason to believe that this condition is permanent. But we need to focus our efforts better, and to invest more resources in this struggle. As the famous Holocaust survivor, and namesake of our Center, Simon Wiesenthal wrote in 1989, "The combination of hatred and technology is the greatest threat facing mankind.")[13] How we face that threat might well define the world we will live in the near future.

Ms. HARMAN. Thank you very much. And thank you for that set of recommendations.

Since the votes have not been called, I think we will now show the video prepared by Ms. Katz. Do you want to say anything about this before we tee it up?

Ms. KATZ. No. Just think that this is a small portion that people see on a daily basis. This is just a very small sample of what you get to see on a daily basis as an individual who joins any of these message boards. Thank you.

[Video played.]

Ms. HARMAN. Thank you very much. No votes have been called, so we will begin a round of questions. And I will yield myself 5 minutes. We will then go to Mr. Dent, out of order, at Mr. Reichert's request.

I would like to thank all of you for sharing your expertise with us, and note that each of you has brought a very unique point of view to this hearing; from Bruce, who has studied this question across the board, to Ms. Katz, who has done something incredibly unusual, which is to herself infiltrate some of these groups, to Ms.µAftab, who focuses on how to prevent all of our kids from getting caught up in this, and to Mr. Weitzman, who came forth with a series of constructive suggestions. Each of you has added enormously to our hearing record.

I am just curious, as a parent, Ms.µAftab, I just would ask you, what are the chances, if there is a way to assess this, that any of our kids could get caught up in this?

Ms. AFTAB. Madam Chairwoman, the odds are higher than we thought because—and I offer some of my teen experts to testify. They have testified before Congress before to talk to you from their perspective. But so many of our young people are looking for a cause. So many of them feel isolated. And it is very easy, if they find this online, to be drawn into it.

When I go to schools—I talk to 10,000 teens and pre-teens a month in person. When I go out there, I get questions all the time about certain misinformation sites, the MartinLutherKing.org site where they come to me and tell me things about Martin Luther King that are not true, or question the Holocaust. If they are buying that and willing to talk to me about that, they are buying these other things as well. My last name, Aftab, is Middle Eastern. My father was from Iran, so I will sometimes get questions about that as well.

Our children are vulnerable. They are connected. They are connected to, listening to people online more than they are to people offline. And I suspect we are going to be seeing even more of that as they move forward.

[13] Simon Wiesenthal, *Justice Not Vengeance,* Grove Weidenfeld, New York, 1989, p. 358.

Ms. HARMAN. Thank you. And I am going to ask one question of Ms. Katz and then call on Mr.µDent, because I know that he is on a tight time frame.

Ms. Katz, thank you for that video. One of the people talking in your video was Adam Gadahn, the young man I mentioned in my opening remarks, who was radicalized in Orange County, California, the son of Jewish parents; who, as I understand it, was surfing the Web, got to a mosque and, through that mosque, gained the views and the instinct to commit violence and now is in Pakistan as the, I guess he would be the communications representative of Osama bin Laden. I mean, it is a pretty amazing story. Could you address him and others that you have seen and just give us a little more color about what happens in these groups? You mentioned that becoming radicalized in this way is one of the most addictive, interactive and informative experiences of the lives of these people. That is a truly scary statement.

Ms. KATZ. Very much that is the case basically. You join any one of these message boards, and it fulfills all of your needs. I mean, I have seen people get married through the message boards. And the people never met, but you find what you are looking for. The case of Adam Gadahn is really a case that he was a teenager when he first went on the Internet, a son of a Catholic and a Jew from California, who went on the Internet and was recruited, initially was converted because of what he saw on the Internet. Eventually, handlers of al-Qa'ida made him join al-Qa'ida. And to me, he presents one of the dangerous elements that we are facing today as Americans in this society. Using individuals like Adam Gadahn, who lived in this country, was part of this community, using his own life experience to describe how great it is to be part of al-Qa'ida and listening to his messages, which are in English, and they are coming quite often. Just this year, we had about three messages from him, as you could see, with unbelievable quality; messages in English. Who is he speaking to? He is speaking to our American or let us say English speakers. This is a new phenomena, a new trend coming from al-Qa'ida. They don't need Arabic anymore. They want the English speakers along with the Arabic speakers. But Adam Godahn's video is circulated everywhere on the Internet, not only this video, but every video he releases. They make sure that it makes it to YouTube and everywhere else that people can see. He speaks in English. He provides his own stories in his statement about his life in LA and how bad his life experience was until he found al-Qa'ida. Now, part of his messages are so—using our own words, everything that that man keeps on doing against us basically explaining, "you know, being with al-Qa'ida, we are not trying to kill you; all we are trying to do is to live at peace; it is you are the terrorists, you are trying to"—and to me, as a teenager—and the bottom line is you see that a lot of the people we mentioned today who were recruited to the Internet or part of the Internet are young, are very, very young, and it is easy to influence these people, especially when they see someone like Adam Gadahn.

Ms. HARMAN. Thank you very much. I now yield for a question to Mr. Dent. I would note for members that there are four votes on the floor, although this clock does not for some reason signal

that. And following his question and the answer, we will adjourn for these four votes. It should take a maximum of half an hour and hopefully less. And I will return, and I hope other members will return for additional questions.

Mr. Dent.

Mr. DENT. Thank you, Madam Chair. Real quickly. What can we do to go on the offensive? In other words, are we doing enough to create false Web sites and then try to track people who, extremists, who would try to go onto those sites? Are we doing any of that? In other words, create some problems for them that, knowing if they go on these sites, that they may not be authentic and maybe turn the Internet into a less reliable source of information. Is there anything we are doing there that you are aware of?

Ms. KATZ. I don't think a lot is being done. I don't think there is any straight policy, a structure of how you would like to see the Internet in 10 years. Al-Qa'ida has their own future plans. Now, when you come and you set up a message board, a fake message board to attract people—I know that other governments have done that, like Jordanians or the Saudis, Egyptians, in order to attract people, collect IP addresses, gather information. You know, when you are part of al-Qa'ida network, it is not that easy to cheat you basically and to send you to any of these message boards. In my testimony, I literally describe how the online al-Qa'ida message boards are set. There is a very clear structure within the password al-Qa'ida messages that are called the Al-Fajr Center. And you know when you go on these message boards that I showed those are part of al-Qa'ida.

Ms. AFTAB. There is a way to manipulate popular Web sites and profiles. And our government agencies are doing that in some respects, moving certain videos up in the ranking and lower in the ranking. We are also seeing a lot of other sites that are designed to make fun of these sites. And bringing humor to it, you are seeing an awful lot of Arabic centric humor that is designed to discredit some of this. Some of it, I suspect, is being done through governmental agencies. Some of it is done through talented teens who think it is funny. In addition, a lot of this information is tracked, and that information is held, even though it may not be accessed by the social networks; YouTube, MySpace, FaceBook, all of them collect the IP address of every comment and everything posted on those sites and retain it for at least 3 months to turn over to law enforcement for valid subpoenas. So there is some of this, not enough. We can let our young people know they are being manipulated. And through more of that, I suspect we will have fewer gone.

Ms. HARMAN. Thank you very much. The hearing will be in recess for these four votes. Thank you very much.

[Recess.]

Ms. HARMAN. The hearing will reconvene. My apologies to the witnesses. There are a series of surprising votes on the floor which were not anticipated, the first of which took almost an hour. And so I regret that the hearing was disrupted. I am hopeful that some other members will be able to get back in between votes, as I have. But if not, following my questions, we will adjourn if no one else is here. And I apologize for that because so many members did want to participate.

Let me ask you, Dr. Hoffman, you have focused on terrorism for 30μyears; you have now turned your attention elsewhere. But as you reintersect these issues, especially the stories we have heard from other witnesses about how people get hooked on these Internet sites and how the people who show vulnerabilities on sites are preyed upon, how big an issue do you think this is?

Mr. HOFFMAN. Well, I am still focusing on it, of course, just from an academic respect, but work closely with the government. I mean, it is enormous. I think, exactly as you heard from the other witnesses, it is enormous in two senses. First, it is a very inexpensive means for the terrorists. It is very—they can communicate nearly in real time. But I think the biggest part of this is twofold: One is that these falsehoods and conspiracy theories have now become so ubiquitous and so pervasive that they are believed, so you have almost a parallel truth. And it has become a very effective tool for recruiting people. And the key is that the terrorists now have, in essence, they can direct their messages; as I said in my testimony, they can tailor it to whichever demographic they are attempting to reach. There are terrorist groups that have sites in more than 20 languages, for instance. But the key is, behind all this radicalization and information, and that is what I think sometimes we are at risk in Washington in losing sight of, is that there are organizations behind this process. This isn't an organic—somebody who is a homegrown terrorist—this isn't an organic homegrown process. There are terrorist organizations that are actively and deliberately manipulating, exploiting and in turn harnessing this radicalization in the service of violence, and that is what makes it dangerous.

Ms. HARMAN. Let me just interrupt you there. I mean, homegrown terror in the sense that this effort grooms homegrown terrorists. It is not necessarily spawned by them, but yet it finds them and develops them into violent killers; is that correct?

Mr. HOFFMAN. Yes, absolutely. It is the proliferation. And in the study of terrorism, we have never seen a phenomena like this in the power of the Internet. It is a vacuum that these terrorists and jihadist groups have filled. And as your bill proposes and as these hearings are about, we have done, unfortunately, lamentably little to push back against.

Ms. HARMAN. Well, my thought is, having listened to all of you, to make sure that this commission, if it becomes law, and I am hopeful that it will, has a major focus on studying this phenomena. Does everyone agree that that is a useful thing to do? I see you all nodding. Would anyone like to make a comment about that?

Ms. KATZ. I would like to.

Ms. HARMAN. Yes, Ms. Katz.

Ms. KATZ. Regularly I meet with government agencies from all over the world. I have not met any person that really understood how this works. And if you don't really know how something works, you don't understand how the jihadist operates online, you will never be able to counter the phenomena. The first and most important step in this counter-terrorism world of fighting them over the Internet is to understand how they do things. I can tell you from our own experience, just using open-source methods, we were able to stop suicide bombers in many places in the world where no gov-

ernment agency in the United States or elsewhere had the information. And so to me, in order to be able to have any kind of progress or know what kind of legislation you need to put, you have to understand it. And that is why I think that this panel is very important.

Ms. HARMAN. And by stopping suicide bombers, you mean specific suicide bombers, intervening?

Ms. KATZ. Individuals that were recruited online and announce about their time, that arrive to go for their own journey. And we alerted—in one case, we actually called immediately the FBI, and they said, you know, Rita, we don't know how legal it is for us to go and stop something like that. I said, look, we have the e-mail account; we have information about the individual; let us do something; we don't know where he is going to carry out his attack. It was an English message board. And we were extremely nervous. They did not do anything. We ended up finding the individual in the UK, alerted the Scotland Yard. They found him on the plane heading to Pakistan, stopped him, brought him back. And I think that what this case—it is just one case of many others—illustrates is the fact that we had to play the role of law enforcement agencies because we are monitoring and doing what is needed to be done after studying the Internet instead of having the FBI alerting the British authorities about such a plot.

Ms. HARMAN. Thank you for that.

Mr. Weitzman, you were talking about positive messages that your organization puts on. I think Mr.µDent, before we recessed, was asking what we can do to counter this. Could you give us more specific information about what kind of positive message you put out there and what effect it has on people?

Mr. WEITZMAN. Well, when I say positive message, I mean that a message that is basically countering the counter-history that Dr. Hoffman just mentioned. These people are constructing their own version of reality, full of conspiracy theories, full of doctored videos, things that will both recruit or inflame emotions. They are presenting a one-sided view of Islam, as well as any other religion, as well as many other events in world history. So what we talked about doing and what we did was created one Web site to sort of counter that and bypass the official organs of government and media distribution, and to present to Arabic, Farsi, Indonesia, et cetera, people a basic history or view of Jews and Judaism that would be presented obviously by people who knew the traditions and knew the history, did not get into the politics of a Middle East issue, but was there to sort of try to begin to counter that. We have on the Web site a book that I wrote that is the first refutation in English of The Protocols of the Elders of Zion that was translated into Arabic and is also available on the Web site. The protocols is basically the bedrock, the bible, if you will, of all these conspiracy theories. So this is an attempt to refute the protocols directly each protocol by protocol, and it is now available in Arabic as well. So that is an attempt to reach out. We had a meeting in Indonesia as well with Waheed, one of the leading Muslim leaders of the world, that brought together Jewish, Muslim and Christian leaders in an attempt to again bypass the inflamed rhetoric of the Middle East that reached the largest Muslim population in the world, which is

in Southeast Asia, and so on and to try, by doing that, to present a more calm, positive message that hopefully will get translated into a mass reality.

Ms. HARMAN. And how many people hit on that Web site? How do you get people to go there?

Mr. WEITZMAN. Actually, we had a launch. We had invited people from the Arab media. We had a representative of the Organization of Arab Countries.

Ms. HARMAN. Excuse me just a moment.

Mr. WEITZMAN. We launched the Web site in mid-September. Since then, we have already had a couple of responses, e-mails, that people have written in questions. Some of it is very, what we call hate rhetoric, but some of it is just very open questioning about the items on there. So this is one of the approaches.

If I can comment as well very quickly, the issue that we have in some ways is that we are trying to fight this war with the last war's battles, which is very often a pattern that we see repeated in history. The Internet, because of its globalization, because of all the influences that have been mentioned earlier, is something that requires new strategies and new approaches. And we are very often looking to the old strategies and old approaches for answers.

And lastly, we have also been for the past decade contributing a CD, samples of all the type of material, extremist materials, that can be found out, and we have been distributing this to law enforcement, including the FBI, government officials, and we are happy to continue that type of cooperation in the future.

Ms. HARMAN. Let me just say, I applaud that. I applaud the action that you are taking very much. And I hope you recover your voice very soon.

Ms. Katz, you have done groundbreaking work. It is extraordinary what you have done.

And Dr. Hoffman I am going to continue to count on you wherever you may land next. You are someone whose voice is very, very important.

I apologize to all the witnesses. This next vote, the one that is current, is a 5-minute vote, and it takes grandma here a few minutes to get over there. So with no other members here and no real prospect that this floor action is going to calm down, I adjourn this hearing. I thank you for participating. The hearing is adjourned.

[Whereupon, at 4:26 p.m., the subcommittee was adjourned.]

VerDate Nov 24 2008 13:10 Nov 05, 2009 Jkt 000000 PO 00000 Frm 00048 Fmt 6633 Sfmt 6011 H:\DOCS\110-HRGS\110-83\48978.TXT HSEC PsN: DIANE