

**JIHADIST USE OF SOCIAL MEDIA—HOW TO PRE-
VENT TERRORISM AND PRESERVE INNOVATION**

HEARING

BEFORE THE

**SUBCOMMITTEE ON
COUNTERTERRORISM
AND INTELLIGENCE**

OF THE

**COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES**

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

DECEMBER 6, 2011

Serial No. 112-62

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.gpo.gov/fdsys/>

U.S. GOVERNMENT PRINTING OFFICE

74-647 PDF

WASHINGTON : 2012

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) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas	BENNIE G. THOMPSON, Mississippi
DANIEL E. LUNGREN, California	LORETTA SANCHEZ, California
MIKE ROGERS, Alabama	SHEILA JACKSON LEE, Texas
MICHAEL T. MCCAUL, Texas	HENRY CUELLAR, Texas
GUS M. BILIRAKIS, Florida	YVETTE D. CLARKE, New York
PAUL C. BROUN, Georgia	LAURA RICHARDSON, California
CANDICE S. MILLER, Michigan	DANNY K. DAVIS, Illinois
TIM WALBERG, Michigan	BRIAN HIGGINS, New York
CHIP CRAVAACK, Minnesota	JACKIE SPEIER, California
JOE WALSH, Illinois	CEDRIC L. RICHMOND, Louisiana
PATRICK MEEHAN, Pennsylvania	HANSEN CLARKE, Michigan
BEN QUAYLE, Arizona	WILLIAM R. KEATING, Massachusetts
SCOTT RIGELL, Virginia	KATHLEEN C. HOCHUL, New York
BILLY LONG, Missouri	JANICE HAHN, California
JEFF DUNCAN, South Carolina	
TOM MARINO, Pennsylvania	
BLAKE FARENTHOLD, Texas	
ROBERT L. TURNER, New York	

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*

KERRY ANN WATKINS, *Senior Policy Director*

MICHAEL S. TWINCHEK, *Chief Clerk*

I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PATRICK MEEHAN, Pennsylvania, *Chairman*

PAUL C. BROUN, Georgia, <i>Vice Chair</i>	JACKIE SPEIER, California
CHIP CRAVAACK, Minnesota	LORETTA SANCHEZ, California
JOE WALSH, Illinois	BRIAN HIGGINS, New York
BEN QUAYLE, Arizona	KATHLEEN C. HOCHUL, New York
SCOTT RIGELL, Virginia	JANICE HAHN, California
BILLY LONG, Missouri	BENNIE G. THOMPSON, Mississippi (<i>Ex Officio</i>)
PETER T. KING, New York (<i>Ex Officio</i>)	

KEVIN GUNDERSEN, *Staff Director*

ALAN CARROLL, *Subcommittee Clerk*

STEPHEN VINA, *Minority Subcommittee Director*

CONTENTS

	Page
STATEMENTS	
The Honorable Patrick Meehan, a Representative in Congress From the State of Pennsylvania, and Chairman, Subcommittee on Counterterrorism and Intelligence	1
The Honorable Jackie Speier, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Counterterrorism and Intelligence	3
WITNESSES	
Mr. William F. McCants, Analyst, Center for Naval Analysis:	
Oral Statement	6
Prepared Statement	7
Mr. Andrew Aaron Weisburd, Director, Society for Internet Research:	
Oral Statement	8
Prepared Statement	10
Mr. Brian Michael Jenkins, Senior Advisor to the President, Rand Corporation:	
Oral Statement	13
Prepared Statement	14
APPENDIX	
Mr. Evan F. Kohlmann with Josh Lefkowitz and Laith Alkhouri:	
Prepared Statement	27

JIHADIST USE OF SOCIAL MEDIA—HOW TO PREVENT TERRORISM AND PRESERVE INNOVATION

Tuesday, December 6, 2011

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE,
Washington, DC.

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

Present: Representatives Meehan, Cravaack, Long, Speier, and Higgins.

Mr. MEEHAN. The Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence will come to order. The subcommittee is meeting today to hear testimony regarding the emerging threat of the use of social media by terrorists.

I note that we expect there to be votes some time after 3:00, 3:30, and we will do our best. We are very grateful for the presence of this distinguished panel and grateful for your important testimony, but we will do our best to work through the testimony and try to get to as many questions as we can.

At this moment, I recognize myself for an opening statement. I want to welcome today's Subcommittee on Counterterrorism and Intelligence hearing on the "Jihadist Use of Social Media." I would like to thank you all for joining us today, and I especially want to thank our panel of witnesses for testifying on this issue.

Over the past year, the subcommittee has been examining threats to the United States homeland from around the world. We began to look at al-Qaeda in the Arabian Peninsula, and an al-Qaeda affiliate in Yemen with a sophisticated media wing led by Anwar al-Awlaki, which included *Inspire* magazine.

We then turned our attention to the tumultuous events in the broader Middle East, and considered how al-Qaeda and other terrorist networks would use the upheaval to their advantage. Later we held hearings on the threat from the terror networks in Pakistan, from Hezbollah's operations in the Western Hemisphere and then last week on the emerging threat from Nigeria's Boko Haram.

One common theme throughout all of these hearings was that terrorist networks are spreading their message, recruiting sympathizers, and are connecting operationally on-line.

For years, terrorists have communicated on-line, sharing al-Qaeda propaganda or writing in on-line forums dedicated entirely

to the prospect of Islamist terrorism. But they have recently evolved with technological changes, utilizing social media sites such as Facebook and YouTube to enhance their capabilities. The same place the average person posts photos and communicates with family and friends are being used by enemies to distribute videos praising Osama bin Laden.

Terrorists also disseminate diatribes glorifying the murder of innocents and even make connections with each other intentionally or internationally to plot attacks. In the case al-Awlaki, jihadists live on virtually even after they have been physically removed from the battlefield.

Prior to entering Congress, I served as the United States attorney in eastern Pennsylvania. Shortly after my tenure ended, a local woman by the name of Colleen LaRose was arrested on her return to the United States as part of a terror plot that targeted a Swedish cartoonist.

LaRose would later become known to the world as Jihad Jane. However, what is less well-known to the world was she received that moniker because it was the name that she employed on-line, where she became a committed jihadist.

She enthusiastically posted and commented on YouTube videos of supporting al-Qaeda and their allies, but her enthusiasm for jihad went beyond watching videos and offered moral support as well. She made contacts on-line with other jihadis, solicited funding, and orchestrated an actual terror plot.

Her case is a shocking example of how easy it can be to find jihadi content on-line and make operational connections with others who speak aspirationally about violent acts of terror against the homeland.

The Jihad Jane case is not the only one. Only a few weeks ago, Jose Pimentel was arrested for preparing bombs to use in attacking targets in New York City. Before his arrest, Mr. Pimentel had been active on-line. He ran a blog, held two YouTube accounts, and operated a Facebook profile, all dedicated to jihadi propaganda.

In a case that illustrates terrorist recruitment in the homeland via social networking, in December 2009 a group of five men in Washington, DC were arrested in Pakistan for attempting to join militants fighting along the border with Afghanistan. Later to become known as the Virginia Five, they were reportedly contacted by a Taliban recruiter through YouTube after one of the members of the group praised an on-line video showing attacks on American troops.

These examples highlight the emerging challenge posed by terrorists engaging on-line. The internet was designed to ease communication, and it must stay that way. However, we cannot ignore the reality that we have been unable to effectively prevent jihadi videos and messages from being spread on popular social media websites like YouTube and Facebook.

I have called this hearing today to learn more about what has been done and what must be advised as we move forward.

Another central issue I would like to learn more about is whether or not social media websites can become useful sources of intelligence in our fight against terrorism. On-line movements are

traceable, nowhere more often so than on social networks which are designed to make connections among people much easier.

I believe the intelligence and law enforcement communities can use this open information to combat terrorism and other crimes. However, it is essential that civil liberties and individual privacy be appropriately protected. I am encouraged by recent remarks made by Under Secretary for the Office of Intelligence and Analysis, Caryn Wagner, where she indicated that the Department of Homeland Security will be working to enhance its ability to monitor social media for threats against the homeland, and I look forward to learning how that may be done as she develops these procedures.

With that, I look forward to hearing from today's witnesses, and I would now like to recognize the Ranking Member, the gentlelady from California, Ms. Speier.

Ms. SPEIER. Mr. Chairman, thank you for holding this hearing and for your continued cooperation. I would also like to thank the witnesses for being here today and look forward to gaining some insights from you on how terrorists use our social media and how the power of social media can be used for both countering the narrative used by terrorists and effective information sharing of potential terrorist activity.

Social media is the No. 1 activity on the world wide web, we know that, accounting for over 22 percent of all time spent on-line in the United States. For instance, Twitter averages about 200 million tweets per day, Facebook boasts about 800 million active users throughout the world. Social media spreading messages to many users at one time is commonplace and their power has proven to be remarkable.

When it comes to looking at the power of social media, we must look to the Arab Spring. As the Arab Spring ensued, social media spread messages to which the world subscribed, followed, tweeted and retweeted. For instance, the week before Egyptian President Hosni Mubarak's resignation, the total rate of tweets about political change in Egypt ballooned ten-fold. The top 23 videos featuring protests and political commentary had nearly 5½ million views. More than 75 percent of people that clicked on embedded Twitter links about the Arab Spring were from outside the Arab world.

Social media become a megaphone that disseminated information and excitement about the uprisings to our outside world. The users of social media in the Middle East caused the world to take notice and to witness the revolution. Social media enabled these revolutionaries, change agents in their own right, to spread their messages beyond national borders to all corners of the world.

Knowing the power of social media and its reach, it is quite natural that terrorists groups themselves would try to use social media to their advantage. For example, we know that former al-Qaeda in the Arabian Peninsula leader, Anwar al-Awlaki, was known to some as the bin Laden of the internet. The late al-Awlaki used various social media such as Facebook, blogs, and YouTube videos to try and recruit and develop a cadre of terrorists in the United States.

We know that al-Awlaki used on-line videos to praise those who not only perpetrated violent acts against people in the United

States such as Major Nidal Hasan but also those who waged unsuccessful attacks such as the attempted Christmas Day Bomber. We also know that the attempted Times Square Bomber, Faisal Shahzad, was in contact with al-Awlaki via e-mail.

What we do not know is how many people have actually been radicalized by viewing blogs, news feeds, and tweets by al-Awlaki and others like him that espouse violent ideology. At what point do those influenced by terrorist ideology over the internet become real, live terrorists?

Terrorists acts by design are intended to create fear or draw attention to their message regardless of whether the message is hatred for a particular group of people, a government, or a policy. Terrorists, through their actions, also have the agenda of causing economic disruption. Just by their menacing and prompting the government to take action and extend its financing can sometimes be a win for them.

Hence, who is the real audience for terrorists on the internet? Is the government who terrorists may feel will spend its money and energy chasing when it finds potential leads, or is it for those that terrorists really feel may be led to espouse their ideology and eventually act upon it?

Since we understand the power of social media as effectively used in the Middle East, what can we do to empower users of social media to counter the message terrorists spread? I am eager to learn today how people can be encouraged to use social media to spread the message that America is not a Nation that is fearful, but a Nation that is abundant with ideas, expression, and innovation.

We know that a vigilant public can provide essential information to law enforcement that thwarts terrorist activity. For example the attempted Times Square bombing by Faisal Shahzad was prevented by law enforcement who received tips of suspicious activity in the area. Are there ways that social media providers can partner with the government to mitigate terrorist activities on their sites without the fear of strict regulation and censorship? How do we encourage the public to utilize these platforms to act as our eyes and ears?

Since social media are such valuable information-sharing tools, is it possible for law enforcement to use social media to share trends and concerns that may threaten our communities, educate the public on how to report suspicious activities, and develop new partnerships with the community?

Is it possible for social media to be used on levels that would actually affect the scope of our intelligence gathering? For example, a few months ago, the Afghan Taliban exchanged tweets with NATO in Kabul during an attack. Can social media present unique opportunities for counter-messaging and direct engagement with terror groups that our Government is currently overlooking?

I am eager to hear from the witnesses how social media can be used to counter the messages espoused by terrorists. I am looking forward to hearing how social media can be used to share information, how users can be assured that by sharing information they will not give up their Constitutional rights. With social media being such powerful tools, what steps are companies, users, and

law enforcement taking to effectively thwart terrorists activities? What more should we be doing?

I have many more questions, Mr. Chairman, but with that I will yield back.

Mr. MEEHAN. Thank you, Ranking Member Speier. Other Members of the committee are reminded that opening statements may be submitted for the record.

So we are pleased to have a distinguished panel of witnesses before us today on this very, very important topic. I would like to first introduce William McCants. He is an analyst at the Center for Naval Analysis where he focuses on al-Qaeda, terrorism, and Middle Eastern policies. He is also an adjunct faculty at Johns Hopkins Krieger School. From 2009 to 2011, Mr. McCants served as the senior adviser for countering violent extremism in the Office of the Coordinator for Counterterrorism at the U.S. State Department. I will bet you didn't get that title on one card.

Prior to that he was the program manager of the Minerva Initiative in OSD policy, an analyst at the Institute for Defense Analysis and a fellow with West Point's Combating Terrorism Center. McCants is the founder of Jihadica.com, a group blog that explains the global jihadi movement. The blog has been featured on the cover of the *New York Times* and rated by Technorati as one of the top 100 blogs on global politics. *Wired Magazine* recently described it as the gold standard in militant studies. McCants is an editor of the *Militant Ideology Atlas* and author of a forthcoming foreign affairs article on al-Qaeda. This fall Princeton University Press is publishing McCants' book, *Founding Gods, Inventing Nations*.

I next turn to Mr. Andrew Weisburd, and he has been engaged in counterterrorism and the collection, analysis, and dissemination of intelligence since 2002, primarily focused on the use of the internet by al-Qaeda and other Islamist extremist organizations and movements. He has been a provider of expert services to a variety of organizations since 2003 and has engaged in research for organizations such as NATO and the United States Department of Justice.

He is a long-time contract instructor in the practitioner education program at the Combating Terrorism Center at West Point and regularly provides training and briefings to the FBI and CIA. He has a BS in information systems from Southern Illinois and an MA in criminology, and he has written various books and included a chapter for the FBI Counterterrorism Division textbook on comparing jihadi and street gang videos on YouTube.

Last, Mr. Brian Michael Jenkins is a senior adviser to the President of the RAND Corporation and is the author of *Will Terrorists Go Nuclear?* and several Rand monographs on terrorism-related topics. He formerly served as chair of the Political Science Department at RAND. In anticipation of the 10-year anniversary of 9/11, Jenkins spearheaded the RAND effort to take stock of America's policy reactions and give thoughtful consideration of the future strategy. That effort is presented in *The Long Shadow of 9/11: America's Response to Terrorism*. I thank you for forwarding a copy of that and I found it very—I recommend it as reading to anybody who is considering the analysis of what has happened over the last course of the decade from a variety of different topics.

Very, very provoking. Commissioned in the infantry, Jenkins became a paratrooper and a captain in the Green Berets. He is a decorated combat veteran, having served in the 7th Special Forces Group in the Dominican Republic and with the 5th Special Forces Group in Vietnam. He returned to Vietnam as a member of the Long Range Planning Task Group and received the Department of the Army's highest award for service.

In 1996, President Clinton appointed Jenkins to the White House Commission on Aviation Safety and Security. He is a research associate at Mineta Transportation Institute, where he directs continuing research on protecting surface transportation from terrorist attacks.

So I thank all of our panelists. I know this is a complex topic, and there is a lot to be said, so I will ask if you will do your best to summarize your written submitted testimony and focus on those issues which you think are the most important things for us to hear in your written testimony and appreciate as well that we will have time for questions. So thank you, Mr. McCants, and I now recognize you for your testimony for 5 minutes.

STATEMENT OF WILLIAM F. MCCANTS, ANALYST, CENTER FOR NAVAL ANALYSIS

Mr. MCCANTS. Thank you, Chairman Meehan, Ranking Member Speier, Members of the committee. I appreciate the opportunity to testify today on the ways al-Qaeda supporters use social media. Most of the research on the subject is confined to discussion forums, an older form of social media that allows users to comment on topics that interest the group.

Al-Qaeda forum users are usually anonymous. The links between them are unknown, and the administrators heavily moderate the discussions. There are only a handful of these fora and the most prominent of them only numbers 50,000 members, many of whom have multiple accounts or, like Aaron and I, are researchers, passively watching. Participating on the forums may harden the views of al-Qaeda supporters and it may push them to take action, but no one is being radicalized on them. They are already members of the radical choir singing to one another.

If the internet does play a role in radicalization, it is happening elsewhere. Sometimes recruiters fish for susceptible youth on mainstream websites, sometimes youth find the content themselves on sites like YouTube, led to it out of curiosity or following the trail of their own conviction. They then share what they find with their acquaintances on social networking sites like Facebook. Thankfully, the vast majority of youth who watch and read al-Qaeda propaganda are either unaffected or choose not to act.

As tested recently by one anonymous on-line recruiter he posited that if you post al-Qaeda propaganda to all of the mainstream websites, only .00001 percent of the people who viewed it would go out to fight for al-Qaeda and even fewer would carry out suicide operations. By his reasoning that is 10,000 people out of a population of 1 billion Muslims. Those numbers might be a bit off, but I don't think by much. We are talking about a relatively small number of people.

Since most people are already fireproofed against al-Qaeda's call to action, the U.S. Government should focus on putting out the fire of criminal activity rather than removing the incendiary material. Follow the smoke trail of al-Qaeda propaganda, looking for those who celebrate its content and distribute it intensively for the purpose of recruitment. Chances are that some of them will do something criminal.

As you might surmise from my testimony, I do not put much stock in closing on-line user accounts held by people that do not violate our laws. I also do not put much stock in intervening with well-meaning outreach programs or removing propaganda. There are too many downsides to these approaches. They are also unnecessary. The FBI and local law enforcement in the United States have done a fair job in finding al-Qaeda supporters on-line and arresting them before they hurt anyone. They have gotten very good at following the smoke trails and putting out the fire of criminal activity.

However, as social networking on-line becomes more private and confined to one's acquaintances, this will be increasingly difficult to do. For legal and technological reasons, it is harder to get access to information on corporate-owned sites like Facebook compared to al-Qaeda-owned forums. Working through these issues is outside of my area of expertise, but I would close by again emphasizing that the first priority should be monitoring and not taking down content. Focus more on following the smoke and looking for the fires of criminal activity and focus less on removing incendiary materials since most people are already fireproof.

Thank you for your time.

[The statement of Mr. McCants follows:]

PREPARED STATEMENT OF WILLIAM F. MCCANTS

Thank you, Chairman Meehan, Ranking Member Speier, and Members of the committee. I appreciate the opportunity to testify today on the ways al-Qaeda supporters use social media.

Our understanding of how the internet creates al-Qaeda supporters is limited by where we look. With few exceptions, most of the research on the subject is confined to discussion forums, an older form of social media that allows users to comment on topics that interest the group. Al-Qaeda forum users are usually anonymous, the links between them are unknown, and the administrators heavily moderate the discussions. Everyone on these forums is either a stalwart supporter of al-Qaeda or analysts who passively watch. There are just a handful of these forums, and the most prominent of them only numbers 50,000 members, many of whom have multiple accounts or are researchers like me. Participating on the forums may harden the views of al-Qaeda supporters and push them into taking action but no one is being radicalized. They are members of the choir singing to one another. For those of us watching, we see only the finished radicalized product and not the process that produced it.

So where and how are al-Qaeda supporters initially radicalized on-line? The where question is easier to answer than the how: Sometimes recruiters fish for susceptible youth on mainstream websites. Sometimes youth find the content by themselves on sites like YouTube, led to it out of curiosity or by following the trail of their convictions. They then share what they find with their acquaintances on social networking sites like Facebook. In the so-called "Five Guys" case, there is a mix of both trends. Young men in the D.C. area watched al-Qaeda videos on YouTube and shared them with one another. A Taliban recruiter contacted them through YouTube and facilitated their travel to Pakistan.

As the Five Guys case suggests, al-Qaeda supporters use a mix of social media to watch and spread the organization's propaganda on-line. Some of these sites, like Facebook, are a goldmine for analysts because they show the users' connections. But they can also be more difficult to penetrate compared to the anonymous discussion

forums. A friend request from a stranger is unlikely to be answered in the affirmative. Because these more closed social networking sites are effective at transmitting propaganda, we may yet see the day when an al-Qaeda video is solely distributed peer-to-peer without announcement on the anonymous discussion forums, thus eluding the media and researchers but nurturing the radicalized.

Thankfully, the vast majority of youth who watch and read al-Qaeda propaganda are either unaffected or choose not to act, as attested recently by one anonymous on-line recruiter. He posited that if you post al-Qaeda propaganda to all of the mainstream websites, only 10% of the people will likely look at it. Of those, only 10% will like what they see. Of those, only 10% will embrace the idea of jihad. Of those, only 10% will propagandize for it. Of those, only 10% will go out to fight in a jihad. And of those, only 10% will seek martyrdom. By his reasoning, 10,000 people out of a population of one billion Muslims, or 0.00001%, would go out to fight for al-Qaeda and even fewer would carry out a suicide operation. Those numbers might be a bit off but not by much. We are talking about a relatively small number of people.

Because the number of people is so small, it is difficult to say why some become active supporters of al-Qaeda and others do not. What we can say is that the vast majority of people who watch and read al-Qaeda propaganda will never act violently because of it. Put metaphorically, the material may be incendiary but nearly everyone is fireproof. Since that is the case, it is better to spend our resources putting out the fires and issuing warnings about the dangers of fire rather than trying to fireproof everyone or remove incendiary material.

Extending the fire metaphor a bit, how do we know where the flames are? We look for smoke. In this case, the smoke is the distribution and celebration of al-Qaeda propaganda. People who celebrate al-Qaeda propaganda on-line and who distribute large amounts of it on mainstream websites for the purposes of recruitment should be watched. Chances are that a few of them will decide to do something stupid, like Zachary Chesser, a recent Muslim convert from the D.C. area who was active in on-line recruitment and was arrested while trying to go fight for al-Shabaab in Somalia.

As you might surmise from my testimony, I do not put much stock in closing on-line user accounts that do not violate our laws. I also do not put much stock in intervening with well-meaning outreach programs or removing propaganda. There are too many downsides to these approaches. They are also unnecessary. The FBI and local law enforcement in the United States have done an excellent job in finding al-Qaeda supporters on-line and arresting them before they hurt anyone. They have gotten very good at following the smoke trails and putting out fires.

I would be willing to revise my approach to on-line radicalization if the data warranted it. But there is little research to go on, which is striking given how data-rich the internet is. In hard numbers, how widely distributed wasawahiri's last message? Did it resonate more in one U.S. city than another? Who were its main distributors on Facebook and YouTube? How are they connected with one another? This sort of baseline quantitative research barely exists at the moment. Analysts are either focused on studying the content of the propaganda or absorbed in stopping the next attack by known militants.

Until this research is done and demonstrates conclusively that al-Qaeda's on-line propaganda is persuading large numbers of people to act on its behalf, I believe the conservative approach I outlined is best, particularly since we have not seen a great increase in foiled plots and arrests. The U.S. Government should focus on watching those people who are actively distributing and celebrating al-Qaeda propaganda on-line, looking for criminal behavior or attempts to connect with active militants. Conversely, the U.S. Government should put much less emphasis on stopping people's exposure to al-Qaeda propaganda since it is not creating many supporters and it is difficult to stop its distribution. In other words, focus less on fireproofing and removing incendiary material and focus more on following the smoke and putting out fires.

Thank you for your time.

Mr. MEEHAN. Thank you, Mr. McCants.
I now turn to Mr. Weisburd for your testimony.

**STATEMENT OF ANDREW AARON WEISBURD, DIRECTOR,
SOCIETY FOR INTERNET RESEARCH**

Mr. WEISBURD. Good afternoon, Chairman Meehan, Ranking Member Speier, Members of the committee. Thank you also for this

opportunity to appear here today to discuss the threat posed by jihadist use of social media.

The next home-grown violent extremist who either attempts a terrorist attack or who is arrested before they can do so will be someone I already know something about. Assuming they have a YouTube account, they will likely be within 2 degrees of separation of someone who has similarly either attempted a terrorist attack or has been arrested on terrorism charges. The following examples help to illustrate this point.

Taimour al-Abdaly launched an attack in Stockholm, Sweden. Mr. al-Abdaly had connections to Arid Uka. Arid Uka opened fire on a bus full of U.S. service personnel at the airport in Frankfurt, Germany killing two. Arid Uka was connected on-line through YouTube to Abu Khalid Abdul-Latif. Mr. Abdul-Latif is awaiting trial. He is accused of plotting with friends to attack a U.S. military facility in Seattle, Washington. Mr. Abdul-Latif had friends in common with Jubair Ahmad. Mr. Ahmad of Woodbridge, Virginia pled guilty to one count of material support for terrorism at the end of last week. He had made a video under the direction of Lashkar-e-Taiba, and he uploaded that video for Lashkar-e-Taiba to YouTube.

Mr. Ahmad had connections to one Mr. Elkhadir Atrash. Mr. Atrash was arrested in northern Israel. He was arrested on charges of organizing a home-grown al-Qaeda cell based there. Not only were all these people connected to each other, but they were also connected to networks, known networks of extremists and/or terrorist organizations.

Turning to terrorist media itself and specifically the videos, the single most common element to these videos is violence. Half of all terrorist videos contain explicit deadly violence. The effects of exposure to this violence are profoundly negative. The deciding factor, however, in determining or—the deciding factor in whether that exposure contributes to future violent behavior is context. The context in which these extremists experience this violence is not merely supportive or permissive of violence, it presents that violence as absolutely essential. It is precisely that kind of context that *Inspire* magazine sought to provide. For the home-grown violent extremists, however, who were targeted or reached out to by Anwar al-Awlaki and Samir Kahn of *Inspire* magazine, each release of *Inspire* magazine was more than just the content. Each new edition of *Inspire* magazine was celebrated as though the release of the magazine itself was an event, a terrorist attack. While we will be dealing with the content of *Inspire* magazine for some time to come, this string of victories is over. Neither Anwar al-Awlaki nor Samir Khan are easily replaced.

Regarding the videos again and regarding the issue of counter-measures of what we might do about them, I don't believe that Google, operator of YouTube, has an interest in promoting violent extremism, and they have already made some effort to address this issue. I will note, however, that authenticity is of great importance to extremists. Each terrorist media product bears a trademark of the associated organization. These trademarks of terrorism are signs of authenticity and are easily recognized, not only by extremists but also by service providers. I would suggest the objective of

not driving all terrorist media off-line, but to marginalize it and to deprive it of these clear indications of authenticity.

Chairman Meehan, Ranking Member Speier, I would like to conclude by thanking you for your service, for your leadership on addressing this issue, and I would be happy to answer any questions you may have.

[The statement of Mr. Weisburd follows:]

PREPARED STATEMENT OF ANDREW AARON WEISBURD

06 DECEMBER 2011

Good afternoon, Chairman Meehan, Ranking Member Speier, and Members of the committee. Thank you for the opportunity to appear before the committee today to discuss the nature and threat posed by Jihadist use of social media.

INTRODUCTION

I have been investigating terrorist use of the internet for roughly 10 years.¹ For the past 2 years, I have analyzed the YouTube accounts of al-Qaeda supporters who have attempted a terrorist attack, or have been arrested on terrorism charges. What I find most alarming is that each time I look at someone new, I find I already have data on them as a result of their being part of the same global community of extremists.

TWO DEGREES OF SEPARATION

Taimour al-Abdaly launched a complex attack on Stockholm, Sweden. He was killed when one of his bombs detonated prematurely.² He used Facebook primarily to keep in touch with family, with one exception. That exception was a known associate of American al-Qaeda operative Samir Khan.³ Al-Abdaly was also an avid consumer of al-Qaeda and related extremist videos, as well as of nasheeds—a cappella songs that celebrate violent jihad and death by martyrdom. However, he made little use of YouTube for social networking, a fact that may reflect some amount of training in operational security.⁴

Taimour al-Abdaly was connected to Arid Uka,⁵ a young man who opened fire on a busload of U.S. military personnel at the airport in Frankfurt, Germany, killing two. Particularly in the case of homegrown violent extremists, terrorism seems to be as much an expression of an identity as of ideology, and the internet provides an ample supply of imagery, music, and text from which the aspiring terrorist can assemble their identity. In the case of al-Abdaly and Uka, the common element was the nasheed.⁶ They shared the same supplier—an as yet unidentified individual, most likely also in Europe, who was well-known to other extremists on account of his work as a curator of extremist songs. The choice of the word supplier is deliberate, and there is a similarity to be seen with drug dealing. Such suppliers link many of the extremists I have studied. They are people who have acquired a reputation on-line of having an ample supply of “the good stuff,” generally videos, audio files (e.g. nasheeds), and literature, all of an extremist nature.

Arid Uka was connected to Abu Khalid Abdul Latif, who is alleged to have plotted with friends to attack a military facility in Seattle, Washington.⁷ They were linked through multiple individuals on YouTube who all associated with a highly radicalized Salafist organization operating in Cologne and Frankfurt, Germany.⁸ The organization, Die Wahre Religion, is led by Ibrahim Abou Nagie, who is currently under indictment for inciting violence and calling for the destruction of other religions.⁹ Abdul Latif represents a not uncommon type of extremist activism on YouTube. His channel served as a virtual pulpit from which he preached regularly

¹A significant portion of that work finds expression on the internet Haganah blog (internet-haganah.com), the site of SoFIR (sofir.org), and now the internet Haganah Forum (forum.internet-haganah.com) and on Twitter (@webradius).

²<http://internet-haganah.com/harchives/007103.html>.

³<http://internet-haganah.com/harchives/007132.html>.

⁴<http://internet-haganah.com/harchives/007107.html>.

⁵<http://internet-haganah.com/harchives/007251.html>.

⁶<http://internet-haganah.com/harchives/007194.html>.

⁷USA v Abdul Latif & Mujahidh, complaint available at http://s88179113.onlinehome.us/2011-06-25/USA_v_Abdul-Latif_et-al%20Complaint.pdf.

⁸<http://forum.internet-haganah.com/showthread.php?146>.

⁹<http://www.taz.de/Anklage-gegen-Hassprediger/!77963/>.

in video sermons that almost no one came to hear. As he began to move forward with his plot, his comments on other YouTube channels became increasingly shrill,¹⁰ yet he stopped short of saying anything that might have warranted opening an investigation. While his words may not have clearly indicated terrorist intent, Abdul Latif was linked via YouTube to a well-known network of homegrown violent extremists here in the United States.¹¹

Abdul-Latif had friends in common with Jubair Ahmad of Woodbridge, Virginia, who has been charged with being a member of Lashkar-e-Taiba, and making videos for that designated terrorist organization.¹² The common link was once again individuals associated with Die Wahre Religion.¹³ Ahmad's alleged membership and direct communications with a bona fide terrorist organization is not something one often sees in open sources of intelligence. His work as a curator of Lashkar-e-Taiba videos appears to be what led to many extremists to link to him (and likely also brought him to the attention of the FBI).

Jubair Ahmad had connections to Elkhadir Atrash, who was arrested on charges of organizing a homegrown al-Qaeda cell based in northern Israel.¹⁴ Like Ahmad, Atrash was a supplier, curating YouTube videos of two extremist clerics, Abu Nur al-Maqqisi of Gaza, and Abu Muhammad al-Maqqisi of Jordan.¹⁵ In addition to Jubair Ahmad, Atrash was connected to a broad range of homegrown violent extremists in the United States, throughout Europe, and in Australia.¹⁶ There is no evidence that extremists must progress through on-line activism to involvement in real-world terrorist activity. Generally it seems there is interplay between the two realms. Nevertheless, Atrash is representative of extremists who engage in on-line activism while toiling away at the more laborious task of assembling a cell that can engage in terrorism, or making the connections necessary to travel to some field of jihad.

These al-Qaeda supporters—part of a global network whose number I estimate at a few thousand—were all connected within two or three degrees of each other on YouTube. The connections between them should be assumed to be weak, rather than strong, but that is not to say such weak ties are unimportant.¹⁷ While a terrorist cell will be composed of strongly-tied individuals, it will be from within a weakly-tied community that they emerge. Weak ties are the paths along which information flows, including militant ideology, and intelligence regarding both potential targets for terrorism as well as counterterrorism activities. Conversely, the weakness of strong ties is that information no longer flows effectively. In the life-cycle of terrorist movements and organizations, one sees again and a again a particular process: Successful counterterrorism activity, generally in the form of arrests and prosecutions, causes communities of extremists to fracture. Weak ties break, leaving the strongly tied units with fewer sources of support and intelligence. This makes them more vulnerable to counter-terrorism, and the process repeats itself.¹⁸

MEDIA, COMPUTER-MEDIATED COMMUNICATIONS, AND VIOLENCE¹⁹

Terrorism—violence for political aims—requires a steady output of media for the movement to remain relevant, to maintain morale, and to recruit new members. For the terrorist organization or movement, the low cost and ease of access of the internet make it an ideal channel for the distribution of terrorist media. Terrorism is also a social phenomenon. Individuals may act alone, but in almost all cases, the terrorist is a product of a community of extremists. The genuine lone wolf is extremely rare. Because of their political and social needs, social media sites are very attractive to violent extremists. But this fails to explain how the combination of people, media, and technology contributes to the problem of homegrown violent extremism.

Computers affect how we experience media and how we interact with others. Extremists are as susceptible to these effects as we are. The on-line environment is

¹⁰ <http://internet-haganah.com/harchives/007379.html>.

¹¹ *Ibid.*

¹² <http://www.fbi.gov/washingtondc/press-releases/2011/woodbridge-man-charged-with-providing-material-support-to-terrorist-organization>.

¹³ <http://internet-haganah.com/harchives/007423.html>.

¹⁴ <http://forum.internet-haganah.com/showthread.php?150>.

¹⁵ *Ibid.*

¹⁶ <http://internet-haganah.com/harchives/007426.html>.

¹⁷ For a discussion of weak and strong ties, see “The Strength of Weak Ties” by Mark S. Granovetter, *The American Journal of Sociology*, Vol. 78, No. 6 (May, 1973).

¹⁸ The history of the decline and fall of the German R.A.F. is a classic example of these processes at work.

¹⁹ For a thorough review of these issues, see *Jihad, Crime, and the Internet* by Erez Weimann, and Weisburd, NIJ2006-IJ-CX-0038 (in press), pp. 21–30.

immersive. We feel we are in a place, often called cyberspace. When we are on a social media site, we feel that we are virtually together with our friends, family, and comrades in arms. We feel we are present in the videos we watch. On-line interaction brings people closer, faster. On-line relationships get off to a strong start, and then move off-line if possible. In the case of two people seeking a soulmate, the result may be a happy union. In the case of aspiring terrorists, the result may be less positive. On-line social networks tend to mirror off-line social networks. People—extremists included—use social media to keep in touch with people they already know. An individual's ability to get involved in terrorism is directly related to who they know, and this is precisely what social media sites reveal to us. The benefits of this to law enforcement are enormous.

In terrorist media, the single most common element is violence.²⁰ Half of all terrorist videos contain explicit, deadly violence. The effects of exposure to such violence are profoundly negative. The deciding factor in whether that exposure contributes to future violent behavior is context. The context in which extremists experience terrorist media is not merely supportive of violence—it presents violence as absolutely essential.

SAMIR KHAN, ANWAR AL-AWLAKI, AND INSPIRE MAGAZINE

Each new edition of *Inspire* was celebrated as a victory, as an attack in itself. In that sense, the deaths of al-Awlaki and Khan can only help in the battle against homegrown violent extremists. There will be no more such events to celebrate. Neither of them is easily replaced, and in the event the magazine is re-launched, it is worth noting that the work involved in producing the magazine likely contributed to the successful targeting of al-Awlaki. Finally, information does not preserve itself in perpetuity on the internet. If *Inspire* magazine remains available for download, it will only be because activists continue to upload it, and every upload of *Inspire* magazine is an event that will leave a trail, and is an act that—in light of the content of the magazine—can likely be investigated and prosecuted.

COUNTERMEASURES

The U.S. intelligence community is already making very effective use of the internet to identify and investigate extremists. Some additional actions can contribute to undermining the processes that enable extremists to engage in violence.

Producing and distributing media for Foreign Terrorist Organizations constitutes material support for terrorism. I would argue that a service provider who knowingly assists in the distribution of terrorist media is also culpable. While it is in no one's interests to prosecute internet service providers, they must be made to realize that they can neither turn a blind eye to the use of their services by terrorist organizations, nor can they continue to put the onus of identifying and removing terrorist media on private citizens. I don't believe that Google, operator of YouTube, has an interest in promoting violent extremism, and they have already made some effort to address this issue, but they can and should do more.

Branding in terrorist media is a sign of authenticity, and terrorist media is readily identifiable as such due to the presence of trademarks known to be associated with particular organizations. The objective should be not to drive all terrorist media off-line, but to drive it to the margins and deprive it of the power of branding, as well as to leave homegrown extremists unable to verify the authenticity of any given product.

CONCLUSION

Chairman Meehan and Ranking Member Speier, I would like to conclude by thanking you for your service and for your leadership in addressing this issue.

I would be happy to answer any questions that you may have.

Mr. MEEHAN. Thank you, Mr. Weisburd. I now turn to Mr. Jenkins for your testimony.

²⁰Ibid., and Comparison of Visual Motifs in Jihadi and Cholo Videos on YouTube by A. Aaron Weisburd (2009), in *Studies in Conflict and Terrorism*, 32:12 1066–1074.

**STATEMENT OF BRIAN MICHAEL JENKINS, SENIOR ADVISOR
TO THE PRESIDENT, RAND CORPORATION**

Mr. JENKINS. Thank you, Mr. Chairman and Ranking Member Speier, Members of the committee, for inviting me to talk to you about this important subject.

Although all terrorist groups use the internet, al-Qaeda is the first to fully exploit the internet and the social media. This reflects some unique characteristics of al-Qaeda itself. It regards itself as a global movement that therefore requires a global network of communications to support it. It sees its mission as not simply one of creating terror but one of awakening the Muslim community. Its leaders regard communications as 90 percent of their struggle and therefore, despite the security risks, these leaders communicate regularly with video and audio messages.

These are distributed on the official websites, and then they are redistributed in a vast number of additional websites, but beneath this there is a tier of forums that allow for direct participation by on-line jihadists so they can become part of the movement themselves.

Al-Qaeda leans on these cybertactics out of necessity. U.S. counterterrorist operations plus unprecedented international cooperation among the intelligence services and law enforcement organizations of the world have degraded al-Qaeda's operational capability.

As a consequence, al-Qaeda today is more decentralized, more dependent on its field commands, its affiliates, its allies and above all on its ability to inspire home-grown terrorists. In this connection, al-Qaeda has embraced individual jihadism and has emphasized do-it-yourself terrorism. That is a fundamental shift in strategy.

Many would-be jihadists begin their journey on the internet seeking solutions to their personal crises, validation of their anger, the thrill of clandestine activity. Of these, a few move beyond the internet to seek terrorist training abroad or to plot terrorist attacks here, but overall the response in America to al-Qaeda's intense marketing campaign thus far has not amounted to very much.

Indeed, between 9/11 and the end of 2010, a total of 176 persons, Americans, were identified as jihadists; that is, accused of providing material support to one of the jihadist groups or plotting terrorists attacks. In fact, despite years of on-line jihadist exhortation and instruction, the level of terrorist violence in the United States since 9/11 has been far below the terrorist bombing campaigns of the pre-internet 1970s.

This suggests a failure of al-Qaeda's strategy. It indicates that not only are America's Muslims rejecting al-Qaeda's ideology, not only is this a remarkable intelligence ascent, but there are some inherent weaknesses in this on-line strategy.

Al-Qaeda has created a virtual army which has remained virtual. Although its strategy depends on individual initiative, it offers on-line participants the means of vicariously participating in the jihadist struggle without incurring personal risks. Indeed, the expression of convictions, of commitment, of threats and boasts becomes not a summons to arms but, in fact, a distraction from action in the real world, a kind of psychologically satisfying video game. Therefore we are not seeing the threat yet.

What does this mean in terms of a response? As the two previous witnesses have indicated, this on-line discussion and these postings are a source of valuable intelligence. So rather than devoting vast resources to shutting down content and being dragged into a frustrating game of whack-a-mole—as we shut down sites, they open up new ones. Instead, we probably should devote our resources to facilitating intelligence collection and criminal investigations so that we can continue to achieve the successes that we have had thus far in identifying these individuals, uncovering these plots and apprehending these individuals.

[The statement of Mr. Jenkins follows:]

PREPARED STATEMENT OF BRIAN MICHAEL JENKINS¹

DECEMBER 6, 2011

IS AL-QAEDA'S INTERNET STRATEGY WORKING?²

Terrorists use the internet to disseminate their ideology, appeal for support, spread fear and alarm among their foes, radicalize and recruit new members, provide instruction in tactics and weapons, gather intelligence about potential targets, clandestinely communicate, and support terrorist operations. The internet enables terrorist organizations to expand their reach, create virtual communities of like-minded extremists, and capture a larger universe of more-diverse talents and skills.

While almost all terrorist organizations have websites, al-Qaeda is the first to fully exploit the internet. This reflects al-Qaeda's unique characteristics. It regards itself as a global movement and therefore depends on a global communications network to reach its perceived constituents. It sees its mission as not simply creating terror among its foes but awakening the Muslim community. Its leaders view communications as 90 percent of the struggle.

Despite the risks imposed by intense manhunts, its leaders communicate regularly with video and audio messages, which are posted on its websites and disseminated on the internet. The number of websites devoted to the al-Qaeda-inspired movement has grown from a handful to reportedly thousands, although many of these are ephemeral. The number of English-language sites has also increased.

Al-Qaeda's communications are a distributed effort. Its websites fall into three categories: At the top are the official sites that carry messages of the leaders. Recognized jihadist figures discuss issues of strategy on a second tier. The third tier comprises the many chat-rooms and independent websites where followers verbally and visually embellish the official communications, fantasize about ambitious operations, boast, threaten, and exhort each other to action.

The quantity and easy accessibility of these sites have attracted a host of on-line jihadists, some of whom are technically savvy and contribute their skills to the overall communications effort.

The jihadist enterprise has created on-line magazines such as *Inspire* and has recruited hometown communicators—native-born Americans, including al-Qaeda's Adam Gadahn and Anwar al-Awlaki, and al Shabaab's Omar Hammami—who understand American culture and can communicate in a way that will appeal to young American Muslims. Those seeking more direct dialogue can work through the internet to exchange messages with jihadist interlocutors.

Al-Qaeda leans on cyber tactics as much out of necessity as for efficiency's sake. U.S. counterterrorist operations have pounded on al-Qaeda's central command degrading its operational capabilities, while unprecedented cooperation among intelligence services and law enforcement organizations world-wide has made the jihadists' operating environment increasingly hostile. As a result, al-Qaeda today is

¹The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to Federal, State, or local legislative committees; Government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a non-profit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

²This testimony is available for free download at <http://www.rand.org/pubs/testimonies/CT371.html>.

more decentralized, more dependent on its field commands and affiliates and on its ability to inspire local volunteers to carry out attacks.

Al-Qaeda has embraced individual jihad as opposed to organizationally-led jihad. Increasingly, it has emphasized do-it-yourself terrorism. Those inspired by al-Qaeda's message are exhorted to do whatever they can wherever they are. This represents a fundamental shift in strategy. As part of this new strategy, al-Qaeda has recognized on-line jihadism as a contribution to the jihadist campaign. Despite some grumbling from jihadist ideologues about on-line jihadists not pushing back from their computer screens to carry out attacks, the threshold for jihad has been lowered. Action remains the ultimate goal but on-line warriors are not viewed as less-dedicated slackers.

Many would-be jihadists begin their journey on the internet, seeking solutions to personal crises, validation, and reinforcement of their anger, the thrill of clandestine participation in an epic struggle. We have no way of counting the number of on-line jihadists. There may be thousands. Nor can we calibrate their commitment, which can range from merely curious visitor to the most determined fanatic.

Of these, a few have moved beyond the internet to seek terrorist training abroad. Five young American students were arrested in Pakistan for attempting to join a terrorist group—they started their journey on YouTube. Some American jihadists like Zachary Chesser were inspired to set up their own jihadist website. Others like Samir Khan and Emerson Begolly exhorted others on-line to carry out terrorist attacks. Still others have found sufficient inspiration on the internet to plot or carry out terrorist attacks in the United States like Michael Finton, who plotted to blow up a Federal building in Illinois, or Major Nidal Hasan who killed 13 of his fellow soldiers and wounded 31 others at Fort Hood, Texas in 2009. Jose Pimentel apparently radicalized himself on the internet, urged others to carry out attacks, then migrated from encourager to would-be bomber, following instructions from al-Qaeda's *Inspire* magazine to build his explosive devices.

Overall, however, the response in America to al-Qaeda's intense marketing campaign thus far, has not amounted to much. According to my own study of radicalization and recruitment to jihadist terrorism in the United States, between 9/11 and the end of 2010, a total of 176 individuals were arrested or had self-identified as jihadists.³ This includes those arrested for providing material assistance to jihadist groups (Hamas and Hezbollah do not fall into this category), attempting to join jihadist fronts abroad, or plotting terrorist attacks. (Analysts may argue about the inclusion or exclusion of a few cases, but the totals remain small.)

The number of jihadists identified to date represents a tiny turnout among the approximately 3 million American Muslims—six out of 100,000. There is no evidence of evidence of any vast jihadist underground. Most of the cases involve one person.

There was an uptick in cases in 2009 and 2010, owing mainly to recruiting in the Somali community, but the number of homegrown terrorists declined between 2009 and 2010. The current year may show a further decline in the number.

The determination of America's jihadists, with a few exceptions, appears to be low. Of the 32 terrorist plots discovered between 9/11 and 2010, only 10 had what could be generously described as operational plans. And of these, six were FBI stings. Intentions are there—provided with what they presume to be bombs, America's jihadists are ready to kill, but without external assistance, only four individuals attempted to carry out terrorist attacks on their own. Fortunately, most also lacked competence. Only three managed to attempt attacks, and only two, both lone gunmen, were able to inflict casualties. Suicide attacks are rarely contemplated.

Despite years of on-line jihadist exhortation and instruction, the level of terrorist violence in the United States during the past decade is far below the terrorist bombing campaigns carried out by a variety of groups in the 1970s. The absence of jihadist terrorist activity since 9/11 reflects the success of domestic intelligence operations. It also indicates that America's Muslim community has rejected al-Qaeda's ideology. And it suggests a failure of al-Qaeda's internet strategy.

It appears that while internet strategies aimed at creating at least weak ties among a large number of on-line participants offer opportunities to terrorist enterprises like al-Qaeda, such strategies also appear to have inherent weaknesses. They may create virtual armies, but these armies remain virtual. They rely on individual initiative to carry out terrorist actions, but they offer on-line participants the means to vicariously participate in the campaign and please God without incurring any personal risk. On-line jihadist forums may be providing an outlet that distracts jihadists from involvement in real-world operations.

³Brian Michael Jenkins, *Stray Dogs and Virtual Armies: Radicalization and Recruitment in the United States Since 9/11*, Santa Monica, CA: The RAND Corporation, 2011.

This may be a particular weakness of the jihadist movement, which recognizes fervent commitment evidenced by making disruptive threats, urging others to carry out attacks, creating terror, rather than limiting participation to physical terrorist attacks. If 90 percent of the struggle is communications, according to al-Qaeda, then on-line jihadism cannot be disparaged. For the virtual warrior, the opportunity to display one's convictions, demonstrate one's intentions and prowess through boasts, threats, and fantasy attacks on the internet counts as achievement. Al-Qaeda's own pronouncements tend to equate the declaration of intentions with their achievement. They include among their accomplishments what they intend to do. For many young men who grew up with the internet, there is no sharp line dividing the real world from the virtual world—the virtual world is the real world. On-line jihadism, then, may be a distraction from the real thing—not a call to arms, but a psychologically rewarding videogame.

Individual participation in an on-line group as opposed to joining a real group may further undermine action. While some individuals display the resolve to carry out attacks without the reinforcement of peers, the history of terrorist plots suggests that peer pressure plays an important role in driving a conspiracy toward action. On the internet, one can turn off the conspiracy at any time. On-line jihadism is readily accessible but it also offers easy off-ramps.

On-line instruction in terrorist tactics and weapons is important for the jihadists, but extremists learned how to make bombs and carried on bombing campaigns long before the internet. The most serious jihadist plots in the United States have been those in which the conspirators had access to hands-on training abroad, which also appears to have cemented their radicalization.

None of this is to be sanguine about the power of the internet for terrorists. As it attracts more technically savvy participants, on-line jihadism could evolve toward cyberterrorism aimed not merely at defacing government websites, but at physical sabotage of critical infrastructure.

What steps might be taken? Advocates of absolute internet freedom sometimes declare the internet to be beyond any jurisdiction. But it is not self-evident that any attempt to limit on-line hate speech, threats, or incitements to violence will violate the Constitution or destroy innovation on the internet. European democracies impose limits on hate speech. Child pornography is outlawed—it makes no difference how many viewers there are. On-line gambling is controlled. The right to privacy, in my view, does not guarantee anonymity, but caution is in order.

In addition to defining what content should be barred, any effort to limit internet use must realistically assess the ability to monitor and impose the restriction and must obtain international agreement in order to be effective. As Jonathan Kennedy and Gabriel Weimann point out in their study of terror on the internet, "All efforts to prevent or minimize Al Qaeda's use of the internet have proved unsuccessful."⁴ Even China, which has devoted immense resources to controlling social media networks with far fewer concerns about freedom of speech, has been unable to block the microblogs that flourish on the web. Faced with the shutdown of one site, jihadist communicators merely change names and move to another, dragging authorities into a frustrating game of Whack-A-Mole and depriving them of intelligence while they look for the new site. Is this, then, the best way to address the problem?

Government might begin with an assessment of the current actual threat. Al-Qaeda's overall recruiting efforts have not produced a significant result. On-line jihadism is low-yield ore. Cases of real internet recruitment are rare. Appropriate authorities are able to successfully engage in attribution operations as new on-line jihadists emerge, and the FBI has had achieved remarkable success in using the internet to detect conspiracies of one.

A discussion of how American military commands and intelligence agencies wage war in cyberspace lie beyond the scope of this hearing. Theoretically, the strategies may include monitoring on-line chatter, disrupting or infiltrating websites, intervening overtly or covertly to challenge jihadist arguments, even setting up false-front networks to attract would-be terrorists. Meanwhile, the terrorist communications offer a valuable source of intelligence. Instead of legislating restrictions, a more pragmatic approach would aim at facilitating intelligence collection and criminal investigations.

The internet and social media are part of today's battlefield. But as of now, the immediate risks posed by al-Qaeda's on-line campaign do not justify attempting to impose controls that could be costly to enforce and produce unintended con-

⁴Jonathan Kennedy and Gabriel Weimann, "The Strength of Weak Terrorist Ties," *Terrorism and Political Violence*, Vol. 23, p. 203, citing Gabriel Weimann, *Terror on the Internet: The New Arena, The New Challenges*, Washington, DC: US Institute of Peace Press, 2006.

sequences. But as the contest continues, the situation warrants continued monitoring for signals of new dangers.

Mr. MEEHAN. Thank you, Mr. Jenkins, and thanks to each of the witnesses for your insightful testimony. I know you are the ones who have been tracking this activity for some period of time. So I now recognize myself for 5 minutes of questions.

Let me just ask the panel, we have been living with the internet now for some time, and it has expanded and grown. Are these social networks game-changers in any way with respect to the world of terrorism? Or is this just another manifestation, as Mr. Jenkins talked about, with individuals who in some ways are living in a cyberworld of, I think you used the language, virtual reality. I mean how much of the real threat that we are seeing on this communications that is taking place within the world of Facebook and YouTube with a community of those who are wanting to share the message of jihad? Mr. McCants, let me ask you.

Mr. MCCANTS. Thank you. I don't think it is a game-changer in the sense that it is leading more people to become terrorists. Certainly like-minded individuals are finding it much easier to connect with one another, but I don't think we are seeing a rapid increase in their numbers. I agree with the other two speakers. It is a pretty small number.

I will say that it is hard to answer your question with good data and I think this is one of the main problems confronting those who are researching this topic. There is very little quantitative studies that have been done of radicalization on-line, and it is striking given that how quantifiable the internet is.

Mr. MEEHAN. How do you know somebody has been radicalized? That is the difficulty because I think the testimony was that there is a community of individuals that effectively have found themselves and they communicate among themselves, but how do we know where somebody has moved out of the virtual world and into a point which they may carry out an act of jihad, or is it, just as you said, follow the smoke and you might find the ones that go from aspiration to taking actual steps?

Mr. MCCANTS. I think so and I think that is a question that intelligence organizations are better-positioned to answer but for analysts I think you can get pretty far just following the trail of propaganda, looking at its distribution. Much of the focus is on these older discussion forums. I think for a number of the people who study this stuff it is sort of late to come to the realization that a lot of the discussion is shifting toward these more closed social networking sites like Facebook, where it is a lot more difficult to gain access. You can't just make a friend request and expect it to be answered.

So I think it poses a real research problem for analysts on the outside and an intelligence-gathering problem for the U.S. Government.

Mr. MEEHAN. As you answer the questions, Mr. Weisburd, I will turn to you, are we getting to a point where in time those who really do want to, the official folks that want to communicate, do they find sort of this is polluted by all the wannabes that are out there at this point in time?

Mr. WEISBURD. If they found it to be polluted, if the message was diluted sufficiently that might be beneficial to us and detrimental to them. I think though getting back to the point of who is it who is merely aspirational, who is it who is moving to the next step, the internet is only very rarely going to provide you with sufficient indications that that is going on. The internet is not an isolated place. Everything that happens on-line involves people sitting behind a computer screen sitting at the keyboard. So understanding those people and taking investigations, if they start on-line off-line can be an important aid in doing threat assessment, which is really what this all comes down to. We can find extremists on-line. We can find where they are located. But when you have to prioritize with limited resources who you investigate and who you do not or who you apply more resources to and who you do not, indications of how you should do that on-line will be few and far between. It really requires a more holistic view of the person that you are looking at.

Mr. MEEHAN. Mr. Jenkins, you talked a little bit about the do-it-yourself terrorists that are sort of being invited by these forums, driving down to that. Is this the real, I mean the limited threat that we are seeing by virtue of this expansion into the world of social media?

Mr. JENKINS. Thus far it has been. Look, terrorists and ordinary criminals are always going to be ahead of us in exploiting any new technology. Government is always going to be behind on this because we don't invent laws for crimes that haven't yet occurred. So while they move into exploiting new technologies, we have to figure out ways that we can continue to keep up with them.

In fact, your original question, this isn't really a game-changer on this, but we do have to figure out ways that we can keep up with it in terms of our criminal investigations.

Thus far, in terms of trying to separate who is going to go down the path of jihad versus those who are simply going to be, invent an avatar and beat their chests in these various sites about what they would, what they intend to do, thus far the authorities have been pretty good at identifying people and indeed moving them into situations where, in fact, their intentions—

Mr. MEEHAN. One last question because my time is expiring, but are we moving them sometimes? Do we find them and then create the opportunity and then someone almost lures them into taking those next substantive steps that actually turn into purported steps toward acts of terrorism?

Mr. JENKINS. I would hesitate to use the word "lure" because I don't think we want to get into the issue here of entrapment. But certainly by identifying individuals and creating opportunities for them to engage in dialogue with people who they think are al-Qaeda, a number of these terrorist operations that have been uncovered, these terrorist plots, were when individuals thought they had connected with a group. It turned out for them to be the wrong group. Instead of being al-Qaeda it was the FBI. But we can legitimately, I think, probe those intentions and see just how far these people are willing to go.

In most cases, although we don't have, we don't have numbers of dropouts, we have no way of counting those who take the off-

ramp, but those who have followed through turn out again, to echo what my fellow participants here have said, turns out to be a very, very small number. If we are looking for something like whether it is .00001 percent or add a zero or subtract a zero, that is still a very tiny number. That also means, however, that it is an investigative challenge.

Mr. MEEHAN. Thank you, Mr. Jenkins. I now turn to the Ranking Member, Ms. Speier for her questions.

Ms. SPEIER. Mr. Chairman, thank you, and thank you to our witnesses. I was pleasantly surprised by the consistency of your testimony today, because I was expecting, frankly, that there would be a fair amount of discussion seeking to have these various sites taken down. But almost to a person you have said basically that these are tools for law enforcement to use, that it would be far more problematic to take them down than to leave them up and that for the most part these aspirants to the extent that they are don't come to it via the internet, they are already there and then just get confirmation of what they believe. Is that a fair statement, would you say?

Mr. JENKINS. You know, look, it is not as if the internet is not a vector of an al-Qaeda infection. Instead the individuals come to it as seekers. They are looking for something and therefore they search through these sites and find sites that resonate with their belief. The internet will put them in touch with other people. It will make them a part of a broader community, an on-line community. It will reinforce their radicalization. But by itself, the internet doesn't get them all the way there. In fact, one thing I think is important here, a lot of the plots that are being discovered are conspiracies of one individual. It is when people had the requirement that they actually—before the internet, actually had to meet other people, we know in looking at the history of these plots that peer pressure, face-to-face peer pressure plays an important role. It doesn't have the same power on the internet, as I say, because you can turn it off whenever you want to. So you can in a sense play at jihadism and you are not propelled by that face-to-face peer pressure.

So the ability to participate as an individual, even the on-line instruction, while it is important, in the Pimentel case it is important, at the same time, again if you look at the most serious plots, the most serious plots had at least one individual that had hands-on training. So in terms of action, it is still face-to-face contact and hands-on training that gets people all the way there.

Ms. SPEIER. Okay, so having said that, let me ask each of you this question. Is there anything that should keep us up at night relative to the internet as a source of jihadist fomentation?

Mr. MCCANTS. No. We are just not seeing the numbers that would warrant that kind of worry. Again, if there were better research based on good data showing that there were a large number of people that were being swayed by this propaganda, that would cause me worry, and you would want to monitor their activities, but I don't think we even see reason, have reason to believe that a large number of people are even being swayed much less going the extra step of taking action.

Ms. SPEIER. Mr. Weisburd.

Mr. WEISBURD. I find the idea that on my laptop I have information that I will find out after the fact is tied to, I will have some link between somebody who is involved in terrorism who I already know is connected to somebody I didn't know. I find that I have got a few thousand people out there who some among them are almost certain to become involved in terrorism. Who among them is it? I don't know. I really can't tell from looking on-line who is going to be the next shooter of a bus full of servicemen, for example.

On the other hand, I think what all of this revolves around is that involvement in terrorism is complicated. We tend to, I think, underestimate how difficult it is. There are many different factors that need to come into play in order for somebody to successfully get involved in terrorism and there seem to be very many inhibitions, things that get in the way of people becoming involved in terrorism. This is good news for us. I think if we were going to study the issue, the area to study is not so much what is it that enables somebody to become involved in terrorism, but what is it that keeps so many other people from not getting involved in terrorism, not even proceeding into terrorism when they are already what we call radicalized. That I think for us is a more productive way to proceed.

Ms. SPEIER. Thank you. I yield back.

Mr. MEEHAN. Thank you, Ranking Member Speier. Now I turn to the gentleman from Missouri, Mr. Long.

Mr. LONG. Thank you, Mr. Chairman. Mr. McCants, you were talking about most people are fireproof now to zero zero zero zero, and you recommend to put out the fire first. How do you go about putting that fire out as far as—I mean, is this the type of thing the FBI is involved in, that it is doing now?

Mr. MCCANTS. Yes, sir. That is exactly what I mean. I think it is their job to identify where this material on-line is being most intensively discussed and distributed to figure out who is behind those discussions and that distribution and then to watch them, watch them carefully to see if they are going to connect with people that are engaged in actual criminal activity or if they may decide like a Zachary Chesser from this area to go off and fight for a terrorist organization. But they are the ones, at least domestically, who are best placed to keep tabs on what is happening on-line.

Mr. LONG. Following that up, by you are saying that we need better research, and you can research anything on the internet, you can find out how many 6-foot-2, blond-headed, left-handed people, with one blue eye and one green eye go to certain websites. So what is the problem with the research?

Mr. MCCANTS. I think at the moment a lot of the research is either focused on the content of the propaganda or it is focused on people that are already about to engage in criminal activity and the sort of thing I am interested in is finding that smoke trail. For example, Ayman Zawahiri comes out with a statement, I think he did so recently, just track it on-line, figure out which forums has it gone to, who has been sharing it with one another—

Mr. LONG. Why is that difficult? Like I say, why is the research so difficult?

Mr. MCCANTS. I don't think the research is difficult. It's a matter of having the manpower and the interest in doing it. So far, that has been lacking.

Mr. LONG. Okay. Then Mr. Weisburd, *Inspire* magazine, is it deceased along with al-Awlaki, or is it still a publication?

Mr. WEISBURD. The name *Inspire* magazine can certainly be revived. It would probably require somebody in al-Qaeda in Arabian Peninsula giving permission at least for that to happen since it was their product. But *Inspire* magazine was really the culmination of some years of work both on the part of Mr. Al-Awlaki and the part of Mr. Khan. As I said, neither of these gentlemen is easy to replace. The skills required to produce, to gather together the content to turn out a magazine on a regular basis are nontrivial. Certainly the hardware, the computers that they using to produce it for all I know were in the vehicle they were in when it was hit by the missile. So you have none of the little bits and pieces that turn out to be a magazine at the end of the day.

It could be revived. I don't believe it would be the same because of the quality of the personnel who were involved in the original incarnation should there be further incarnations of it. But as a thing in itself and as an expression of al-Awlaki and Khan and what they were doing, as I said, that *Inspire* magazine is deceased.

Mr. LONG. Al-Awlaki will be so difficult to replace, and I have heard that before from other people in testimony, but what is your assessment? Why will he be as difficult as it seems? He is pretty high-profile, and what was unique to him that would prevent something like that from happening in the future?

Mr. WEISBURD. He was particularly good at taking the core message of what they describe as a global jihad and synthesizing it and sort of speaking directly to his followers in plain terms and language they could understand. You hear that response from the people who followed him, that they listened to Anwar al-Awlaki, and he made everything clear. The rest of it was maybe a little more complicated, but you could follow Anwar al-Awlaki's arguments.

The other thing to remember about al-Awlaki is that because he worked in English first and foremost, his material was accessible to everybody who doesn't read and write and speak Arabic, which is a much larger potential audience for his message because when it comes to people who are say in Indonesia or people who are in Turkey or people who are in Europe or the United States, English becomes the common language, it is the language they use in on-line discourse, it is on English language sites that they gather, it is on English language sites that they collect. Among English-speaking leading jihadists, there really is nobody who comes to mind readily who has quite what al-Awlaki had.

Mr. LONG. Thank you and I yield back.

Mr. MEEHAN. Thank you, Mr. Long. I now turn to the gentleman from New York, Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman. Just a couple of things, one of the most influential forces in the entire world, the Arab Spring of last year, amazingly was an 83-year-old retired professor, former Harvard professor by the name of Eugene Sharp. Eugene Sharp wrote a book called *From Dictatorship to Democracy*. Because of social media, Twitter, Facebook, YouTube, his ideas that

were written and developed over a 20-year period were available to young 20-year-olds, revolutionaries in the streets of Tahrir Square in Egypt. I think the point here is that when you look at social media, Twitter, Facebook, YouTube, these are all commodities. These are tools of collaboration. The only thing that you can't commoditize is the imagination that you bring to these tools of collaboration.

In Tom Friedman's book, *The World is Flat*, one chapter is dedicated to the whole notion, and he says that, the chapter is called 11/9 or 9/11, on 11/9/1989 the Berlin Wall fell. We all know what happened on 9/11. He says in a chapter of this book that in 1999, two airlines were started because of the tools of collaboration, social media, the ability to outsource services that we never knew existed before. One was started by an entrepreneur from Salt Lake City by the name of David Neeleman. He started JetBlue airlines. He outsourced the establishment of a new fleet of jets to an American company called Boeing. He outsourced the financing of his new airline to American financiers in the Southwest. He financed the reservation system to housewives and retirees sitting in their homes in Salt Lake City. You call JetBlue airlines and you are talking to a retiree who is in his living room taking your reservation and built one of the most successful airlines in the history of the world.

But we also know from the 9/11 report another airline was started in Kandahar, Afghanistan by Osama bin Laden. He outsourced the planning of his plot to Khalid Sheikh Mohammed. He outsourced the pilot training to small flight schools in Miami. He outsourced the financing to financiers in United Arab Emirates.

The point is that both airlines were designed to fly into New York City, JetBlue to JFK to bring loved ones together, to promote commerce, to be a force for good in the world, and al-Qaeda into Lower Manhattan to exact a death and destruction beyond human compensation.

The point is that these tools of collaboration are available to everybody, for organization, for aspirational purposes. What matters most and what is most elusive and most difficult to deal with is the imagination that you bring to these tools of collaboration and how do we as a free society best influence whether or not the imagination brought to these tools of collaboration that are available to everybody are for good or evil?

I would just ask you to comment on that.

Mr. JENKINS. It is an interesting comparison although in terms of 9/11, they were able to succeed because the al-Qaeda of that day was a much more centralized enterprise, despite the fact that it outsourced these various components. I mean Khalid Sheikh Mohammed was in al-Qaeda's central core. They had readily accessible training camps that brought from around the world would-be jihadists a continuing talent show from which they could select people for missions. The finances came into a central point. In other words, there was a lot more centrality and coordinating of possibilities in the al-Qaeda of 9/11 than the al-Qaeda of today.

One of the things we have succeeded in doing in 10 years is dispersing those training camps and pounding on that al-Qaeda cen-

tral core and dispersing this. So it is a very different kind of organization today.

Can the these tools be used to attract all sorts of varying talent? Yes. Samir Khan represents a new generation that came along. Anwar al-Awlaki did. If you cast the net broadly, they are—and this is one of the dangers that the internet does propose—you can cast your net very, very broadly. It may be low-yield ore, but you are going to look to bring together some talent here and there.

What they are having difficulty with, however, is still creating or recreating that kind of connectivity that enables them to carry out a strategic operation on the scale of 9/11. So instead we get smaller-scale plots, smaller-scale attacks and, as indicated by one of the other witnesses, even the recognition that failure is a contribution to the cause. Now that is lowering the threshold considerably.

We are going to be dealing with that for a long time. But I think there has been progress in destroying their capacity to carry out these kind of centrally directed operations.

Mr. MEEHAN. Thank you, Mr. Higgins. I turn to the gentleman from Minnesota, Mr. Cravaack.

Mr. CRAVAACK. Thank you, Mr. Chairman. Thank you for the panel, for being here today. I very much appreciate your insight. It seems, and correct me if I am wrong, but it seems at least right now that a social media is more an echo chamber where people that are, like you said, Mr. Weisburd, is kind of just feeding off of each other. Would that be a fair assumption?

Mr. WEISBURD. The jihadist forums in particular as opposed to the later social media sites, say like Facebook or YouTube, the forums are echo chamber, absolutely. Dissenting opinion is simply not allowed. I think the reason why for example YouTube is perceived as something of a risk is that people who are—it is where jihadist content can be put in front of a mainstream audience, and so there is always some concern that this content is going to be appealing to some people who might otherwise not be exposed to it, who have no idea where the jihadist forums are, don't know where to go or cannot get into them. How great a risk that is I think is easily overstated. As Mr. McCants said, people tend to be, as he put it, fireproofed. There are all these inhibitions in terms of getting involved in terrorist activity. So I am not particularly alarmed about it. But I would not think it fair to describe say YouTube as an echo chamber. In terms of countermeasures it is useful to note that as well because unlike on a jihadist forum where I can't confront somebody with their extremism, on YouTube, YouTube is not going to remove people on their website, users of their website because they are too extreme, okay, YouTube is not going to intervene in that. So you have the opportunity to interact with people on a site like YouTube that you don't have on the jihadist forums precisely because YouTube is not controlled by al-Qaeda as opposed to the forums. So there is an opportunity there.

Mr. CRAVAACK. Would both other panelists agree with that?

Mr. MCCANTS. Yes, I would agree. It is striking to me that after 10 years with two wars in the Middle East and all of the turmoil that they have caused such a fertile field for grievance to grow, and the growth of all of this social media for people with these grievances to connect, and yet you still have a very small number of

people who are responding positively to al-Qaeda's message, and of them an even smaller slice that are willing and able to undertake violence. To me that is what is striking about al-Qaeda supporters using social media, is that, yes, they are connecting with one another, but it is such a small number and they are able to undertake such few attacks in this country.

Mr. CRAVAACK. Thank you. Mr. Jenkins, do you feel the same way?

Mr. JENKINS. I would agree with that. Despite the developments we have seen, the dramatic developments in the internet in the last 10, 15 years, and despite this intense retail campaign by al-Qaeda, and even recruiting of native-born communicators who understand an American audience and can communicate in an effective way, they are not selling a lot of cars. I mean, as a marketing operation this is not really working for them, and as I say, it may in fact be a distraction.

Now, that doesn't mean, however, that we ought to be sanguine about the future on this. This is something that requires continued monitoring. One thing that we probably need to be concerned about is that to what extent can they translate those who have a desire to connect via the internet and to do something but not to take the personal risks of carrying out a bombing, what sort of malevolent mischief can they get up to on the internet itself? Can they move from denial of service attacks to, if they go in that direction, can they move in the direction of even sabotage via the internet?

Right now I think that is a bit of a reach, but this is not something that we ignore because we are doing well so far. I think this is something that we have to continually watch, see what the trends are and maintain our ability to try to intercept it going in depending on what direction it goes in.

That doesn't mean shut down sites. What it means is that our intelligence and our ability to operate in this new technological environment has to be equal to theirs.

Mr. CRAVAACK. Thank you for your comments. Moving forward then, what I am hearing from you is that we should monitor the situation and use it as an intelligence-gathering operation. Thank you, sir, and I am out of time. I yield back.

Mr. MEEHAN. Thank you, Mr. Cravaack. I just have one follow-up question myself. Mr. Jenkins, you were talking about an issue which did strike me as you were describing in your earlier testimony the virtual, almost aspirational level in which people can check in and check out of the conversation, but in that virtual world the one connection that we have there is to our infrastructure, to other kinds of things where they are connected to the internet. What is the possibility or likelihood of somebody continuing down that path and playing the game, but for the first time they really are connecting to infrastructure that we have here in the United States?

Mr. JENKINS. I wouldn't be able to comment on the probability of that. That is a question that calls for prophecy. But certainly we have to accept that as a possibility and continue to watch this. If the internet and social media are able to attract a large number of individuals, then there are going to be among that people of diverse capabilities and talents. So there is a possibility in a sense

of if you have that many coming in of a mutation in some direction that could put us off running in a new direction. So we are dealing with fast-moving technology and we are dealing with a large population of individuals most of whom don't strap on bombs to themselves, and that is the positive. But will they find other ways of satisfying their desires to contribute beyond simply talking about this? That is something we want to watch for. So that becomes an intelligence concern as well.

Ms. SPEIER. Maybe just one last question, Mr. Chairman. Based on what you have testified to, do we look at the five guys from Virginia as just being unusual in that it appears that they were radicalized on the internet and then went to Pakistan to seek training, correct?

Mr. WEISBURD. I think the key point of that is that they were five guys who knew each other in the real world and then they were also using the internet. But the fact that there was a group of them who could come together and collectively get it together to go off to Pakistan is the significant part. For one individual to go off to Pakistan to try and go to a training camp would be scary for that lone individual. It requires a lot of courage basically to try and do something that risky. Five individuals can collectively sort of get their act together to go and try and do that. That is really I think the key. That is what you look for in investigations. You are looking for people who have some sort of group, you know who are part of a group that is moving forward, because for an individual to engage in terrorism it is much more difficult than for a group of people. Organizations are much more effective than these disparate groups.

Ms. SPEIER. All right. Thank you.

Mr. MEEHAN. I want to thank the witnesses for your valuable testimony and the Members for their questions. The Members of the committee may have some additional questions for witnesses. We will ask if they do submit those to you, you do your best to respond if you can. The hearing record will be open and held as such for 10 days.

So without objection, the committee stands adjourned. Thank you for your testimony.

[Whereupon, at 3:10 p.m., the subcommittee was adjourned.]

APPENDIX

STATEMENT OF EVAN F. KOHLMANN WITH JOSH LEFKOWITZ AND LAITH ALKHOURI

DECEMBER 6, 2011

THE ANTISOCIAL NETWORK: COUNTERING THE USE OF ON-LINE SOCIAL NETWORKING TECHNOLOGIES BY FOREIGN TERRORIST ORGANIZATIONS

Though the term “social networking” tends to conjure up immediate visions of Facebook and Twitter, the origins of the term are far less humble. In the era before the existence of the internet, social networking was the process of conventional human interaction that took place in key locations like schools, marketplaces, religious centers, and sports events. Consequently, for traditional terrorist organizations like al-Qaeda’s first generation, the critical social networking hubs consisted of secretive guesthouses, a handful of notoriously extremist mosques, and fixed training camps scattered alongside the Afghan-Pakistani border.

In the wake of the September 11, 2001 terrorist attacks on the United States, these conventional hubs were quickly targeted by the United States and its allies. Under overwhelming pressure, training camps were shut down, guesthouses raided, and notorious recruiters jailed. Al-Qaeda Inc. was seemingly put out of business. Yet, as new generations have come of age in the internet era, the al-Qaeda organization has spread its on-line presence, establishing a tenacious beachhead in cyberspace. In the face of constant pressure from U.S. law enforcement and intelligence agencies, al-Qaeda has defiantly organized a cabal of critical jihadi-oriented on-line social networking forums. Likewise, its members, allies, and supporters heavily populate conventional services like YouTube and Facebook. And for those who make contact with groups like al-Qaeda and the Pakistani Taliban through these services, the reality is no less meaningful than having done so in person. This is the primary emerging frontier of al-Qaeda recruitment and financing.

In fact, the word “emerging” hardly captures the reality of what is actually happening right now on the internet. Each week, new internet personalities disappear from the web on a mission to live out their outlandish jihadi fantasies. Flashpoint Global Partners has identified at least 120 such individuals (including U.S. nationals) who have graduated from being mere “pajama-hideen” to taking a real role in terrorist activity over the past 7 years. Of these 120 hardcore extremists, more than half are now dead—killed in a barrage of Predator drone strikes, failed bomb-making activities, and in gunbattles with the U.S. military and various other “infidel” adversaries. The numbers increase dramatically each month. On August 14, 2011, users on the radical “Ansar al-Mujahideen” chat forum were notified that one of their fellow members, “Hafid Salahudeen”, had been killed in a U.S. drone missile attack in Pakistan’s restive Waziristan region along the Afghan border.¹ Only 1 week later, on August 23, 2011, another “Ansar al-Mujahideen” user “Khattab 76” was reported dead after clashes with the Egyptian military in the Sinai Peninsula, where he had gone to “fight the Zionists.”² According to Ansar forum administrators, inspired by what he saw on the web, “Khattab 76” had made several previous failed efforts to join al-Qaeda in both Iraq and Afghanistan.³ On September 18, 2011, moderators on al-Qaeda’s premiere “Shamukh” web forum advised their comrades that user “Qutaiba” had departed for Algeria to join al-Qaeda in the Islamic Maghreb (AQIM). They quoted a final message from him sent over the internet: “I am here amongst the mujahideen in the Islamic Maghreb . . . I advise my beloved

¹ <http://www.as-ansar.com/vb/showthread.php?t=46237>. August 14, 2011.

² <http://www.as-ansar.com/vb/showthread.php?t=46873>. August 23, 2011.

³ <http://www.as-ansar.com/vb/showthread.php?t=46873>. August 23, 2011.

ones to join the convoy before it is too late . . . Your brothers in AQIM are waiting for you.”⁴

Arguably, the most famous individual to self-recruit on the internet using al-Qaeda’s social networking websites was a young Jordanian doctor named Humam al-Balawi (a.k.a. “Abu Dujanah al-Khorasani”). On December 30, 2009, al-Balawi—a former administrator on top-tier al-Qaeda social networking forums—blew himself up at a secret CIA base along the Afghan-Pakistani border.⁵ At the time, CIA and Jordanian intelligence agents believed they had successfully recruited al-Balawi as a double agent to help hunt down Dr. Ayman al-Zawahiri and other top al-Qaeda figures. In fact, al-Balawi was offering a starkly different perspective to his associates on the jihadi web forums. In an interview published on al-Qaeda’s “Al-Hesbah” forum in September 2009, only 3 months previous, al-Balawi appealed, “How can I encourage people to join the jihad while I’m staying away from it? . . . How do I become a burning wick for others follow the light of? Can any sane person accept that? Not me.”⁶ As for al-Qaeda’s social networks, he crowed, “I left behind on the forums some brothers who are dearer to me than members of my own family. When I meet any mujahid here who knows about the forums, I rush to ask him who he knows from al-Hesbah—as he might be one of those whom we loved in the cause of Allah, from amongst the administrators or members, and I would hug him as one brother longing for another.”⁷ These now-prophetic warning signs were ignored by many at the time, who dismissed al-Balawi’s threats as merely inflated internet rhetoric. It came at an enormous cost—seven CIA agents killed, including some of the agency’s top experts on al-Qaeda.

Al-Qaeda itself is well aware of the key role that jihadi web forums are playing in recruiting a new generation of militants willing to sacrifice themselves on its behalf. No longer are internet-based social networks the exclusive domain of aspiring, would-be terrorist neophytes. Indeed, the veteran Yemeni explosives expert accused by the U.S. Government of helping organize al-Balawi’s deadly suicide bombing attack, Hussain al-Hussami, was likewise an active user on the Al-Hesbah on-line forum.⁸ On October 1, 2009, he posted a request on the forum on behalf of “the Jalaludeen Haqqani Organization”: “dear brothers, I have some Shariah and military guides printed in the Russian language, and I want to translate them into Arabic. If you can assist me, whether with software, websites, or translators, may Allah reward you generously.”⁹

Recognition of the brave new world of terrorist communications and recruitment has reached the highest echelons of al-Qaeda. In June 2010, the group released an audio message from Shaykh Mustafa Abu al-Yazid—third-in-command behind Usama Bin Laden and Ayman al-Zawahiri—hailing “my brothers—the shadowy knights of the [jihadi] media, a school whose alumni includes the hero ‘Abu Dujanah al-Khorasani’ . . . and those who remain and continue their efforts and sacrifices” and calling on them “to stand in the trench that Allah has chosen them for their own well-being . . . You are the thundering voice of jihad, its mighty arrows, and its roaring weapons that have caused so much concern amongst politicians at the White House.”¹⁰ Yet, perhaps what is most startling about this phenomenon is the sharp increase in the use of brand-name U.S. commercial social networking services such as YouTube, Twitter, and Facebook by terrorist organizations and their supporters. On password-protected top-tier al-Qaeda web forums, contributors are boasting that “YouTube is among the most important media platforms in supporting the mujahideen, as it is ranked third in the world with more than 70 million daily visitors.”¹¹ This is reflected in the increasing occurrence of hardcore jihadi videos hosted by YouTube as evidenced in Federal terrorism cases.

- On February 1, 2011, Colleen R. LaRose (aka “Jihad Jane”) pled guilty to charges in the Eastern District of Pennsylvania, including conspiring to provide material support to terrorists.¹² LaRose was an unusually prolific presence on YouTube; court documents highlighted a particular posting—under the name

⁴<http://www.shamikh1.info/vb/showthread.php?t=127866>. September 18, 2011.

⁵Oppel, Richard A. Jr., Mark Mazetti, and Souad Mekhennet. “Attacker in Afghanistan Was a Double Agent.” *New York Times*. January 4, 2010.

⁶“Vanguards of Khorasan” Magazine. Vol. 1; Issue 15 (September 2009).

⁷“Vanguards of Khorasan” Magazine. Vol. 1; Issue 15 (September 2009).

⁸Baldor, Lolita and Matt Apuzzo. “Top Al Qaeda Operative Reportedly Killed In U.S. Drone Attack.” Associated Press. March 17, 2010.

⁹<http://www.alfaloja.net/vb/showthread.php?t=86082>. October 1, 2009.

¹⁰As-Sahab Media Foundation. “He Who Equips a Fighter Has Waged Battle Himself, by the Mujahid Shaykh Mustafa Abu al-Yazid-May Allah Accept Him.” First released: June 15, 2010.

¹¹<http://www.alfaloja.info/vb/showthread.php?t=62982>. May 16, 2009.

¹²“Pennsylvania Woman Pleads Guilty in Plot to Recruit Violent Jihadist Fighters and to Commit Murder Overseas”. U.S. Department of Justice Press Release. February 1, 2011.

“JihadJane”—in which she indicated she was “desperate to do something somehow to help” suffering Muslims.¹³

- On February 24, 2011, Northern Virginia resident Zachary Chesser was sentenced to 25 years in prison “for communicating threats against the writers of the South Park television show, soliciting violent jihadists to desensitize law enforcement, and attempting to provide material support to Al-Shabaab, a designated foreign terrorist organization.”¹⁴ According to court filings, “Chesser . . . started his own YouTube.com homepage, utilizing userID LearnTeachFightDie, where he posted videos and hosted discussions. Chesser explained that this name perfectly symbolized his philosophy at the time: Learn Islam, teach Islam, fight for Islam, and die in the name of Islam . . .”. After closing that account, “he then opened a YouTube site utilizing user name AIQuranWaAlaHadeeth.”¹⁵
- Joseph Jeffrey Brice was charged in May 2011 for making and detonating an Improvised Explosive Device—consisting of TATP, APAN, and ANFO—along a highway in Washington State. According to court filings, Brice—who was seriously injured in the blast—set up a YouTube channel that “was used to post videos that depicted the use of explosives. Some of these videos contained the embedded logo of the Al-TawhidWal Jihad (al-Qaeda in Iraq) and a jihad chant soundtrack, known as Nashid . . . two of them depicted the use of explosives in the Clarkston, Washington vicinity.” He also posted numerous comments on YouTube. For example, on January 8, 2011, in response to the shooting of Congresswoman Gifford, he wrote, “. . . as long as it’s one more dead American kuffar, what difference does it make to me if she is a democrat or a gop?” On December 27, 2010, he wrote, “NPED [non-primary explosives detonator] can now be purchased in most states legally through pyrotechnic dealers.”¹⁶
- On December 2, 2011, Virginia resident Jubair Ahmad pled guilty to providing material support to Lashkar-e-Taiba (LeT).¹⁷ According to DOJ, “in September 2010, Jubair produced and uploaded a propaganda video to YouTube on behalf of LeT, after communications with a person named ‘Talha.’ In a subsequent conversation with another person, Jubair identified Talha as Talha Saeed, the son of LeT leader Hafiz Mohammed Saeed. Talha and Jubair allegedly communicated about the images, music, and audio that Jubair was to use to make the video. The final video contained images of LeT leader Hafiz Saeed, so-called jihadi martyrs, and armored trucks exploding after having been hit by improvised explosive devices.”¹⁸

Nor has this phenomenon been limited to the United States. In the United Kingdom, a 21-year-old woman, Roshanara Choudhry, made headlines in May 2010 when she stabbed and attempted to assassinate British MP Stephen Timms at a community center in East London. According to British authorities, “When interviewed by police, Choudhry said she stabbed Mr Timms because he voted for the Iraq war and she wanted to achieve ‘punishment’ and ‘to get revenge for the people of Iraq’.”¹⁹ In her police interview, she explained that she “wanted to be a martyr” because “that’s the best way to die.” She further told the interviewer that she had adopted that perspective after listening to lectures by Yemeni-American cleric Anwar al-Awlaki, killed in a U.S. drone strike in Yemen in September 2011. Asked how she found out about al-Awlaki, she explained, “On the internet . . . if you go on YouTube, there’s a lot of his videos there and if you do a search they just come up. I wasn’t searching for him, I just came across him. I used to watch videos that people used to put up about like how they became Muslim.”²⁰

It is often forgotten that YouTube is not merely a video hosting site, but also a formidable social networking forum. Contributors can draw the attention of reg-

¹³ *U.S. v. LaRose*. Eastern District of Pennsylvania. Criminal No. 10–123. Superseding Indictment. Filed April 1, 2010.

¹⁴ “Virginia Man Sentenced to 25 Years in Prison for Providing Material Support and Encouraging Violent Jihadists to Kill U.S. Citizens.” U.S. Department of Justice Press Release. February 24, 2011.

¹⁵ *U.S. v. Chesser*. Eastern District of Virginia. Criminal No. 1:10mj504. Affidavit of FBI Special Agent Mary Brandt Kinder. Filed July 21, 2010.

¹⁶ Re: 538 Riverview Boulevard No. 3. Clarkston, WA. 99403. Affidavit of FBI Special Agent Leland C. MeEuen. May 6, 2011.

¹⁷ “Pakistani National Living in Woodbridge Pleads Guilty to Providing Material Support to Terrorist Organization.” U.S. Department of Justice Press Release. December 2, 2011.

¹⁸ “Woodbridge Man Charged with Providing Material Support to Terrorist Organization.” U.S. Department of Justice Press Release. September 2, 2011.

¹⁹ “Woman sentenced to life imprisonment for attempted murder of MP”. Metropolitan Police Service Press Release. November 3, 2010.

²⁰ Roshanara Choudhry police interview. Interview conducted on May 14, 2010, in Forest Gate police station.

istered subscribers who then are able to comment on video uploads and communicate back and forth with the original source. Users subscribe to each other's feeds based on mutual interests—in this case, various aspects of al-Qaeda and violent extremism. The process is so efficient and precise that it has repeatedly attracted the interest of the Pakistani Taliban, not merely to spread propaganda, but also to engage in a dialogue with viewers and even recruit those interested in joining a foreign terrorist organization. On December 9, 2009, five young Muslim-American men from the Washington, DC area were arrested by authorities in the Pakistani town of Sargodha. The men were accused of attempting to join al-Qaeda forces on the Afghan-Pakistani border. According to a Pakistani police report quoted by ABC News and the *New York Times*, a Taliban recruiter first made contact with the group via Ahmed Abdullah Minni, who had “repeatedly posted comments on YouTube praising videos showing attacks on American troops.”²¹ The 20-year-old Minni had allegedly “become a regular feature” on YouTube with his campaign of on-line vitriol—so much so that a Pakistani Taliban recruiter known as “Saifullah” took an interest and began writing back to him.²²

The Pakistani Taliban carried on their brazen recruitment campaign using YouTube in May 2010. Within days of a failed car bombing in Times Square, New York by Faisal Shahzad, a naturalized American recruited by the Pakistani Taliban, the group published a video recording featuring its leader Hakimullah Mehsud boasting of its role in the would-be attack.²³ The video was posted by an official Taliban on-line courier “TehreekeTaliban” registered as a contributor on YouTube, who engaged in a back-and-forth discussion with critics and supporters in the comment section on the video. One respondent asked, “what is he saying? Can someone translate?” The courier replied, “subtitles are in English, you can easily understand inshaALLAH.” When another viewer condemned the Taliban for their role in the Times Square incident, “TehreekeTaliban” insisted, “I would recommend you to read Quran again with good translation and . . . to do learn . . . from a good shaykh like Imam Anwar Al-Awlaki. You can download his lectures from net, just search google.”²⁴

As the social networking website Facebook has quickly become a ubiquitous part of many Americans' on-line activity, it too has enjoyed increased significance as an amplifier for violent extremist viewpoints and a way for al-Qaeda supporters to identify each other and build budding relationships. In March 2010, one user on al-Qaeda's then-preeminent “Fallujah Islamic Network” appealed, “the least we can do to support the Mujahideen is to distribute their statements and releases.” He added, “we wish from the brothers to also distribute the statement via Youtube and widely . . . and on Facebook.”²⁵ The user offered a cautionary note about using Facebook: “the suggested method is to always access it via proxy, otherwise you're in danger. Make one e-mail on Yahoo that's dedicated for the [on-line] battle only. After creating the email, register on Facebook under an pseudonym with the email you created, and via which the account will be activated. Search for all the profiles and groups.”²⁶

Like YouTube, the role of Facebook in terrorism investigations can be charted as it increasingly surfaces as evidence in Federal criminal indictments. In December 2010, Baltimore resident Antonio Martinez was charged with plotting to attack an Armed Forces recruiting station in Catonsville, Maryland. As recounted in a press release from the U.S. Department of Justice, “Martinez was arrested . . . after he attempted to remotely detonate what he believed to be explosives in a vehicle parked in the Armed Forces recruiting station parking lot.”²⁷ According to the USDOJ:

“On September 29, 2010, Martinez publicly posted on his Facebook account a statement calling for violence to stop the oppression of Muslims, and that on October 1, 2010, he publicly posted a message stating that he hates any person who opposes Allah and his prophet . . . On October 8, 2010, an FBI confidential source (CS) brought these public postings to the attention of the FBI. On October 10, 2010, in

²¹ Shane, Scott. “Web Posts Began Tale of Detained Americans.” *New York Times*. December 14, 2009.

²² See: “Interrogation Report: Profiles of the Foreigners held”. Abbas Majeed Khan Marwat PSP, ASP/UT SARGODHA. Available at: http://a.abcnews.com/images/Blotter/ht_interrogation_report_091211.pdf.

²³ <http://www.youtube.com/user/TehreekeTaliban>. May 2, 2010.

²⁴ <http://www.youtube.com/user/TehreekeTaliban>. May 2, 2010.

²⁵ <http://www.al-faloja.info/vb/showthread.php?t=105942>. March 6, 2010.

²⁶ <http://www.al-faloja.info/vb/showthread.php?t=105942>. March 6, 2010.

²⁷ “Maryland Man Charged in Plot to Attack Armed Forces Recruiting Center”. U.S. Department of Justice Press Release. December 8, 2010.

response to these postings, the CS began communicating with Martinez through Facebook . . . During Martinez' discussions with the CS over Martinez' Facebook page, Martinez wrote that he wanted to go to Pakistan or Afghanistan, that it was his dream to be among the ranks of the mujahideen, and that he hoped Allah would open a door for him because all he thinks about is jihad."

Additionally, on October 17, 2011, Martinez allegedly posted the following on his Facebook page: "I love Sheikh Anwar al Awalki for the sake of ALLAH. A real inspiration[sic] for the Ummah, I dont care if he is on the terrorist list! May ALLAH give him Kireameen." Court filings further note that his Facebook "Friends" included "two radical Islamist websites affiliated with a radical group called Revolution Muslim: Call to Islam—a United Kingdom-based on-line movement dedicated to the implementation of Sharia law world-wide (as stated on its website); and Authentic Tawheed—a pro-jihad group providing links on its website to materials put out by known terrorists such as Anwar al-Aulaqi."²⁸

There is no doubt that YouTube and Facebook have been making genuine efforts in an attempt to thwart the on-line activities of al-Qaeda supporters and violent extremists. However, a quick search for jihadi videos on YouTube is a fairly compelling demonstration that these efforts have thus far been insufficient in addressing the problem. On-line jihadists have reacted with mirth at YouTube's overly-optimistic strategy of relying on its own users to self-police and help to flag individual illicit contributions. The service has, in fact, added a category to its content feedback flags labeled "Promotes terrorism"—that which is "intended to incite violence . . . This means . . . videos on things like instructional bomb making . . . [or] sniper attacks. Any depictions of such content . . . shouldn't be designed to help or encourage others to imitate them."²⁹ Repeated violations can lead to a user being kicked off YouTube, whose stated policy is that "if your account is terminated you are prohibited from creating any new accounts."³⁰ Nonetheless, there is minimal enforcement of this policy and users with terminated accounts often simply create new accounts under different user names, many of which are only minor variations of their blocked accounts. A user on al-Qaeda's top-tier "Fallujah Islamic Network" instructed his associates in May 2009 that if on-line adversaries start to "search for jihad clips . . . so that users can vote to delete them . . . then we must make them pull out their hair by re-uploading deleted scenes, commenting on them, and supporting them. Remember that YouTube is the biggest media podium, so the jihad videos should appear right in the face of those who enter it."³¹

YouTube and its parent company Google have defended their seeming inability to prevent their video sharing service from being manipulated by al-Qaeda supporters and other violent extremists. According to YouTube, "More than 24 hours of video are uploaded every minute."³² Due to the sheer volume of new videos being posted each day, YouTube asserts it is "simply not possible" to prescreen content³³ and thus relies on its user community to flag inappropriate material. Yet, with this amount of incoming new material, it is equally fanciful to assume that YouTube's user community possesses the subject matter expertise or contextual background to effectively block the spread of violent extremist content. Without some sort of automated filtering process, it does not seem realistic to believe that the use of YouTube by terrorists and jihadi extremists will begin to decrease.

If Google is indeed serious about addressing this problem, the company should start by leveraging its own existing technological solutions to ensure known violent extremist content is not distributed via YouTube. A quick comparison with how YouTube manages copyright violations is instructive. YouTube utilizes a system called "Content ID" whereby "Rights holders deliver YouTube reference files (audio-only or video) of content they own, metadata describing that content, and policies on what they want YouTube to do when we find a match. We compare videos uploaded to YouTube against those reference files. Our technology automatically identifies your content and applies your preferred policy: Monetize, track, or

²⁸ *U.S. v. Antonio Martinez*. District of Maryland. Case No. 10-4761 JKB. Complaint. Filed December 8, 2010 and *U.S. v. Antonio Martinez*. District of Maryland. Case No. 10-4761 JKB. Government Response to Defendant's Motions to Dismiss Indictment and Suppress Statements and Seized Evidence. Filed September 27, 2011.

²⁹ <http://www.google.com/support/youtube/bin/answer.py?hl=en&answer=139838>. Last accessed December 2, 2011.

³⁰ http://www.youtube.com/t/community_guidelines. Last accessed December 2, 2011.

³¹ <http://www.al-falaja.info/vb/showthread.php?t=62982>. May 16, 2009.

³² <http://www.youtube.com/t/faq>. Last accessed December 2, 2011.

³³ Benett, Brian. "YouTube is Letting Users Decide on Terrorism-Related Videos." *Los Angeles Times*. December 12, 2010.

block.”³⁴ Users deemed to be acting in violation of copyright law are “required to attend ‘YouTube Copyright School,’ which involves watching a copyright tutorial and passing a quiz to show that you’ve paid attention and understood the content before uploading more content to YouTube.”³⁵ It is hardly a great jump in logic to apply this same strategy to the large, but hardly unmanageable subset of notorious open-source terrorist propaganda videos—archives of which are maintained by private organizations like Flashpoint Global Partners. YouTube has been able to effectively block the majority of pornographic video contributions, reportedly through the use of specific algorithms; similar algorithms should be developed to stem the flow of violent extremist content.

In a further development, YouTube’s parent Google has recently acquired Pitt-Patt, a Carnegie-Mellon spin-off that is considered to have market-leading facial recognition software.³⁶ This technology can theoretically be leveraged to identify offending video content and user profile photos that match those of known terrorists, leading to at least an automatic flagging—if not full deregistration—of the account. Avatar images featuring depictions of high-profile terrorists, such as Usama bin Laden and Anwar al-Awlaki, or the watermarked logos of groups such as Shabaab al-Mujahideen and al-Qaeda in Iraq, are unfortunately nowadays common on YouTube. However, when paired with the right image recognition filter, these watermarks and avatars can provide a powerful, effective roadmap to identify suspect contributors engaged in illicit activity. Similar technology could potentially also be deployed with similar effect by Facebook, Twitter, and other commercial social networking services beset with infiltration by supporters of violent extremism.

If real progress is to be made towards cleansing on-line social networks of terrorists and their supporters, the U.S. Congress must bring pressure to bear on commercial providers who are themselves being victimized in the process to start acting more like aggrieved victims instead of nonchalant bystanders. While any proposed curbs on the freedom of speech should always naturally give one cause for a moment’s hesitation, in this case, it is unclear why official terrorist recruitment material is any less of an odious concern for YouTube or Facebook than pornography. Unfortunately, current U.S. law gives few incentives for companies like YouTube for volunteering information on illicit activity, or even cooperating when requested by U.S. law enforcement. If such companies are to be trusted to self-police their own professed commitments to fighting hate speech, then they must be held to a public standard which reflects the importance of that not unsubstantial responsibility.



³⁴<http://www.youtube.com/t/contentid>. Last accessed December 2, 2011.

³⁵<http://youtube-global.blogspot.com/2011/04/youtube-copyright-education-remixed.html>. Last accessed December 2, 2011.

³⁶<http://www.pittpatt.com>. Last accessed December 2, 2011.