

# TESTIMONY

---

## Is Al Qaeda's Internet Strategy Working?

BRIAN MICHAEL JENKINS

CT-371

December 2011

Testimony presented before the House Homeland Security Committee,  
Subcommittee on Counterterrorism and Intelligence on December 6, 2011

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 nonprofit 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. RAND® is a registered trademark.



Published 2011 by the RAND Corporation  
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138  
1200 South Hayes Street, Arlington, VA 22202-5050  
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665  
RAND URL: <http://www.rand.org/>  
To order RAND documents or to obtain additional information, contact  
Distribution Services: Telephone: (310) 451-7002;  
Fax: (310) 451-6915; Email: [order@rand.org](mailto:order@rand.org)

**Brian Michael Jenkins<sup>1</sup>**  
**The RAND Corporation**

**Is Al Qaeda's Internet Strategy Working?<sup>2</sup>**

**Before the Committee on Homeland Security  
Subcommittee on Counterterrorism and Intelligence  
United States House of Representatives**

**December 6, 2011**

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.

---

<sup>1</sup> The 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 nonprofit 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.

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

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

The jihadist enterprise has created online 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 worldwide has made the jihadists' operating environment increasingly hostile. As a result, al Qaeda today is 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 online jihadism as a contribution to the jihadist campaign. Despite some grumbling from jihadist ideologues about online 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 online 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 online 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 online 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.<sup>3</sup> 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 agree 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 three 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 online 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.

---

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

It appears that while Internet strategies aimed at creating at least weak ties among a large number of online 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 online participants the means to vicariously participate in the campaign and please God without incurring any personal risk. Online jihadist forums may be providing an outlet that distracts jihadists from involvement in real world operations.

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 online 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. Online jihadism, then, may be a distraction from the real thing—not a call to arms, but a psychologically rewarding videogame.

Individual participation in an online 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. Online jihadism is readily accessible but it also offers easy off-ramps.

Online 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, online 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 online 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. Online 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.”<sup>4</sup> 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 Whac-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. Online jihadism is low-yield ore. Cases of real Internet recruitment are rare. Appropriate authorities are able to successfully engage in attribution operations as new online 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 online 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 online campaign do not justify attempting to impose controls that could be costly to enforce and produce unintended consequences. But as the contest continues, the situation warrants continued monitoring for signals of new dangers.

---

<sup>4</sup> Jonathan 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.

