Countering Internet Extremism

By Mr. Timothy L. Thomas

Editorial Abstract: The author examines the modern informational environment, and introduces the concept of contemporary extremist work as a type of living influence laboratory. He focuses on a specific Web-based counter-ideology example, then presents a methodology to address specific cyber audiences.

Introduction

Unless the US crafts a strategy that stymies long-term ideological radicalization among large numbers of Muslim youth, America's 'long war' against terrorism is likely to be just that.

Several issues of seemingly benign importance eventually emerged as significant activities when the US and its coalition partners went to war in Iraq and Afghanistan in 2003 and 2001. One of those issues was extremists' use of the Internet—that transnational communication device. Warning signs of this emerging capability and its influence on events were observed earlier during the Chechen-Russian conflict in the 1990s and in early 2000. Chechen use of the Web enabled them to win over public opinion in the early stages of the conflict, and secure an information warfare victory.

Extremists' use of the Internet has developed rapidly since the Chechen-Russian conflict. Now they are more creative, and more importantly, more persuasive in their methods to recruit members, gain financial support, and provide proof of success. The extremists' task has been made easier since coalition forces are stationed in countries where their understanding of culture and the means of spreading information is less informed. Extremists, on the other hand, tap into both culture and media methods.

Extremists have demonstrated their military capabilities online (their use of video to demonstrate the effectiveness of improvised explosive devices (IEDs) and sniper attacks against coalition forces come to mind) and in their use of clerics and imams to justify their actions to the Arab world. Internet videos, postings on *You Tube*, recruiting on *My Space*, and other such methods have been effective. Recruiters even hand out CDs and DVDs of key speeches and events, at low or no cost, further supporting this cognitive movement.

The coalition response to these measures has been constant but sporadic in the types of organizations involved. First, there is the usual list of players with information operations expertise that have been involved since the beginning: the 1st IO Command, psychological operations groups, the Joint Information Operations Warfare Command, the National Security Agency, DIA and CIA analysts, US think tanks such as RAND, and many others. Second, there has been a constant effort by non-government and government agencies to relook the problem of extremist organizations for decades now. A host of new measures and efforts have joined this group since 1989:

- In 1989 Ben Venzke developed IntelCenter, which has monitored Al Qaeda and other terrorist movement worldwide both before and after 9/11
- In 1998 the Middle East Media Research Institute (MEMRI) was founded. It monitors and analyzes various trends, to include terrorism, in the Middle East press. It has an Islamist Website Monitoring project
- In 1999 the job of Undersecretary of State for Public Diplomacy and Public Affairs was created (occupied by Charlotte Beers, Margaret Tutwiler, and Karen Hughes, three very powerful but marginally effective undersecretaries, from October 2001-November 2007) to develop a State Department effort to put out the US message to the Arab world, mostly via TV and radio stations
- In 2002 Rita Katz and Josh Devon formed the Search for International Terrorist Entities (SITE) intelligence group, to follow terrorist activities
- In 2003 the US Army developed Counterterrorism Center at West Point, to follow extremist thought by looking at the books terrorists put online
- In 2004-2005 the Defense Department hired contractors such as the Lincoln Group to find stringers to write pro-Western stories
- In 2005-2006, DoD conceived and developed Human Terrain Teams, tasked to interact with the population, to better understand the culture and traditions of the area
- In 2006 an Internet Radicalization Task Force was created at the Homeland Security Policy Institute, to develop a report on how to de-radicalize the Web; the report was delivered to Congress
- Specific websites were developed to combat terrorist use of the Internet such as info@stopterroristmedia.org
- US government elements developed a strategic communications plan.

Some of these groups have been more successful than others. Some merely monitor the situation while others make recommendations to counter extremist use of the Internet.

The difficulty in successfully neutering extremist use of the Internet is evident from our daily experiences. For example, in spite of all of these resources—plus all of the money the west has thrown into information (read Internet) security—an individual known as Irhabi 007, sitting in a room in London in front of a monitor, still operated successfully and was effective until the time of his capture. The advantages of using the Internet (anonymity, use of cut -outs, masking of server use, movement from personal computer to cyber café, etc.) enable extremists to make it very difficult to find them.

This article will examine briefly the environment in which extremists now operate (ideological and technical),

outline what issues we must counter, and summarize/review efforts to date to counter, neuter, or cauterize extremists' use of the Internet by coalition forces and governments worldwide. Progress is being made, but it is uncertain if the restrictions on Western democracies in particular (legal, moral, etc.) and the difficulties in countering Internet advantages will ever be able to fully contain online extremism.

The Environment

Information technologies enable extremists to achieve many goals that would have been unimaginable in the 1970s. These technologies have been used to initiate IEDs, to communicate (via cell phones or on the Internet), to employ high-tech deception operations, to filter news and information for the people of the Middle East, and to influence Western opinion. Such flexibility allows development of new uses as required. Yet the influence aspect of information technologies merits the greatest attention.

Several elements of the environment have changed dramatically since the 1970s, and strongly support an extremist's influence of cognitive activities. First, information laboratories (computers) inhabit our work place, homes, and relaxation stops (coffee shops, etc.). It is here that extremists' influence operations take place. A 'lab' used to be a place in a scientific research organization or a university where one went to test theories and make discoveries using Bunsen burners and microscopes. Entire buildings were assembled to run simulations. The modern day "information lab" consists of a desk or laptop. Experiments can be run on real life situations (via virtual environments like *SIMS* and *Second Life*) and perform much of the work that simulation labs used to do. Images can be manipulated according to the creator's wish or to fit a product. Information labs move the individual from being just a TV, radio, or newspapers information consumer, to being producers, users, and interpreters (through interactions such as blogs) of information that shapes or socializes the followers' world views. Theories are tested and discoveries made that have real world consequences, which may or may not be in line with the common good. Access to these devices empowers an extremist's active operations. One can even use the computer monitor to watch *Al Qaeda TV* right at home.

The labs can explain why, how, when, and even where to fight in an open or anonymous manner. These labs serve as cyber mobilizers for people of like thought, but they cyber mobilize fence sitters as well. This is performed through personal messages or mass circulation Internet journals or papers. The lab is an environment where cultural knowledge of the target audience is vitally important in developing both the technological support and know-how/message appropriate for each target. Information labs in the right hands provide sustenance to the cause, offer meaning to one's existence, provide proof of success, and offer personal examples of heroism and martyrdom. These experimental workshops are the combustion chambers that spawn interest in events, and motivate supporters to extraordinary actions. This is a persuasive form of effects-based operations of the mind.

Persuasion helps counter extremism. (Defense Link)

Second, there is minimal or no cost involved in using tools to shape the environment. In the past, tools used in laboratories were expensive. Now information laboratory tools are available as freeware, or via software packages such as Windows, Movie Maker, and Adobe Acrobat. All can be downloaded at will or purchased at minimal cost. Such applications do not require the expense of a college course to access them, just access to the Web. The systems that run the extremists' experiments were created by others, and provided free of charge.

Extremists not only share our networks but easily exploit them. It would be fair to state that extremists go by the law of "we can use your systems, you can't use ours," as witnessed by extremists' use of *Yahoo*'s free online newsgroups (to distribute communiqués), *MySpace*, and *YouTube* among many others. Stateless information labs bypass censorship and regulations as well as traditional cultural norms of restraint, and do what they can to prevent non-sympathizers from accessing their net niche.

Third, just as plants need fertile soil, the environment must possess a rich and adaptive ideological atmosphere. Without this, it is impossible to fertilize the cognitive aspects of their target audience. Instigators create this atmosphere by developing specific images and messages in their information labs, offering their slanted and prejudiced perceptions of reality to selected target audiences. Sophisticated tools mentioned above make this job easier. Content filters ensure only certain viewpoints are available on some sites. Cognitive activities are sprinkled with warnings about the dangers of "other thoughts or ideologies" to one's soul and afterlife. Al Qaeda and other insurgent groups offer specific and unique ideologies that fit selected organic social movements.

Fourth, the environment is organized differently than in the past. The formation of radical media brigades indicates creation of a new combat space, wherein the rules of civilized news organizations do not apply. For that reason, the propaganda videos and photos are often of a shocking nature

in regard to beheading, throat slitting, and other 'online slaughter' techniques. This new combat space is a cognitive battle space without laws, rules, and regulations—operating via manipulation, filters, and fear.

Further, this environment is a transnational communication and influence network. It empowers anyone with an opinion on anything to post their thoughts, and may be read by one individual or by millions. Revered authority figures such as religious leaders can lead followers to specific websites or postings. However, anonymous postings can also have tremendous impact on entire groups of people, if presented properly (that is, with a message that strikes a nerve in a specific cultural setting). Chatrooms or bulletin boards host the bulk of such postings.

This experimental lab in your living room has other uses as well. It can intimidate or taunt rivals with the click of a mouse, persuade fence-sitters to accept a cause based on the evidence presented, allow access to some information but deny access to other sources, and allow for the social networking of criminals and other extremists. These virtual transnational labs have eliminated much of the need for physical training camps (due to the spread of online training material) and thus inhibit law enforcement agencies from detecting where, and in what form, extremist groups operate.

What Must Be Countered?

To counter terrorist use of the Web, it helps to understand the logic that informs an extremist's use of technology. One could literally examine hundreds of books and speeches. Since the purpose of this work is examining ways to counter an extremist's Internet use of the Internet rather than counter-ideology as a whole, we'll look at only one example. The work of ideologue Abu Musab al-Suri (also known as Mustafa 'Abd alQadir Mustafa Husayn, Umar 'Abd al-Hakim, and Mustafa Setmariam Nassar), is representative of this ideology.

Al-Suri believes jihad must be comprehensive and utilize military, political, media, civil, and ideological tools. First, media resources can be used to establish "resistance blockades" that keep the enemy (Western countries) from corrupting Islamic institutions, organizations, and ideas while radicalizing Muslim masses. Second, in addition to the main platforms of the Internet and satellite TV, al-Suri recommends sending written statements that call on Muslims to join the Global Islamic Resistance; to publish works on military and training curricula (e-mail contact lists, CD-ROMs, DVDs, etc.); to translate works into other languages; and to disseminate scholarly writing that supports the spirit of resistance, including opinions regarding the enemies of jihad.

Al Qaeda on the Web. (Alneda.com)

Obviously analysts should conduct an in-depth study of al-Suri's rhetoric and ideological reasoning instead of the short, truncated list offered here.

With regard to technical issues, Jarret Brachman, Director of Research at the Combating Terrorism Center at the United States Military Academy, West Point New York, listed twelve key aspects of a terrorist's use of technology:

1. Extremist posts of insurgent 'job openings' on the Web
2. Extremist posts of motivational imagery that cyber mobilizes insurgents or wanna-be insurgents
3. Extremist downloads of scripted talking points about religious justifications for waging jihad
4. Breaking news posted from a jihadist point of view
5. Extremist posts of links to attack videos
6. Al Qaeda friendly news cast calls that criticize Arab governments collaborating with Jews and Christians and discuss goals of the jihadi movement or establishment of the Voice of the Caliphate.
7. Mobile Internet services offering selected news content via cell phones.
8. Extremist links to several Al Qaeda magazines containing instructions on communications, tactics, and explosives
9. Extremists links to instructions on jihadi websites on how to use software packages and encryption devices and video editing
10. Computer programmer launches of stand alone Web browsing software that allows searches only on particular sites. These efforts to bound jihadi ideological space by intellectually separating them from other areas of cyberspace allows them to become more dogmatic and isolated
11. Extremist protocol offers on how to safely use the Internet. These countermeasures help identify how other governments penetrate their use of software chat programs (such as Microsoft Messenger and PalTalk) and advise readers not to use Saudi Arabian e-mail addresses but rather use anonymous *Hotmail* and *Yahoo* accounts.
12. Extremist posts on how to use video games to reach the young, and instill in them the hope of reaching extremist goals such as a global Islamic caliphate. The more realistic the game, the less dissonance players feel between the game and the world around them. Video games harmonize reality with the need to catalyze awareness of the Muslim requirement to resist.

To be successful, Coalition members must find ways to counter these uses. Further, we must find ways to counter jihadi-themed books, recruitment, and propaganda materials that can be downloaded via cell phone.

Another good extremist technology reference comes from author Remy Mauduit, editor of the US Air Force's *Air & Space Power Journal* French edition. Mauduit spent five years in

an insurgency and guerrilla leadership position during the 1954-1962 Algerian War, and published a book on insurgency and counterinsurgency based upon his hands-on experience. In 2008 he wrote on the effects-based information battle in the Muslim world, including issues that Westerners must learn to counter—such as the seemingly benign Islamic rhetoric that serves as a cover for nationalist, anti-imperialist, and reformist objectives. Such messages include denunciations of the injustices, corruption, and tyranny that have characterized the reigning oligarchies in the Islamic world.

Methods To Counter Or Neuter Extremists' Use Of The Internet

There is no shortage of ideas on how to counter or neuter an extremists' use of the Internet. Of course, none can be designed to totally eliminate such use. Yet several sources offered below provide differing perspectives on how to counter extremist Internet use.

A 2008 *New York Times* article indirectly offers some methods. Writers Eric Schmitt and Thom Shanker discussed weaknesses of insurgent movements, and while not presented as counteractions, these are easily derived:

1. Muting Al Qaeda messages (ways to do so were not offered)
2. Turning jihadi movements own weaknesses against the movement
3. Illuminating Al Qaeda errors
4. Planting bogus e-mail messages and website postings to sow confusion, dissent, and distrust among militant organizations
5. Amplifying the speeches and writings of prominent Islamic clerics who renounce terrorist violence; persuading Muslims not to support terrorists through messages such as that from Abdul-Aziz el-Sherif, who wrote a book renouncing violent jihad on legal and religious grounds
6. Identifying territory that terrorists hold dear, to include emotional territory such as a terrorists reputation or credibility with Muslims, and damaging that territory
7. Identifying and manipulating or destroying terrorist terrain, which at the moment is the Web
8. Using captured computer hard drives to learn how to develop counter-messages to extremists plans or speeches
9. Releasing seized videotapes showing terrorist brainwashing sessions with children (extremist "camps" for children, hate cartoons, etc.) and training sessions with children teaching them to kidnap or kill
10. Releasing letters that demonstrate poor morale within their organization
11. Looking at a militant's culture, family associations, or religion to determine what dishonors them and undermines their rhetoric on the Web
12. Taking away extremists' popular or theological legitimacy for actions such as the moral legitimacy of using weapons of mass destruction
13. Persuading "extremist support networks" to stop offering assistance to extremists and holding these support networks accountable if they do not
14. Perfecting technical systems that identify the source of unconventional weapons or their components.

A March 2008 effort, attributed only to "US authorities," was "implied" from a post to the Islamist website http://www.al-farooq.net/ (currently hosted by SoftLayer Technologies Inc., Dallas, Texas, USA). In a message posted 27 February, administrators claimed US authorities had contacted both the website administrator and its US host to pressure them to remove jihadi content, saying that if they do not, the site will be shut down. Actually, this can be a very effective way to keep server operators from allowing someone to use their network.

Earlier, in February 2008, Colleen Graffy, Deputy Assistant Secretary for European and Eurasian Affairs, US State Department, was quoted by author Bud Goodall as asserting that the main problem with US public diplomacy is "getting the word out." Successes in the public diplomacy world from Graffy's view include nine elements: a European Union news alert system, a rapid response unit, a streamlined approval process for ambassadors' media appearance requests, new media hubs in Brussels, Dubai, and London, a new TV studio, a European liaison position, a "pre-active" approach to media, a TV adviser position, and a Senior Adviser on Muslim engagement. In spite of this rather broad range of options offered by Graffy, Goodall finds the Deputy's remarks out of touch with US strategic communication needs. His take on the problem is that it is more important to use active engagement through a pragmatic complexity model than to merely 'get visual,' or 'get the message out.'

Marc Sageman, a forensic psychiatrist and former CIA case officer, is recognized for his work on extremist mindsets, and potential ways to influence them. In March/April 2008 he wrote that in the past mobilization occurred by face-to-face networks that caused a small number of people to become extremists. Today, online radicalization substitutes for face-to-face radicalization, allowing extremists to get support and validation. Sageman notes these virtual marketplaces of extremist ideas are the invisible hand that is organizing extremist activities worldwide. The leader of this violent social movement—attracting younger members and now women—is not a person, but "the collective discourse" appearing on half a dozen influential forums. Each network acts according to its own understanding, however, and Al Qaeda Central cannot "impose discipline on these third-wave wannabes, mostly because it does not know who they are." Thus their collective actions do not amount to much. Sageman believes these people thrive only at the abstract fantasy level, making them vulnerable to whatever may diminish their appeal among the young. Thus Sageman sees real opportunity for countering these movements if we construct the correct message, particularly if these separate groups cannot coalesce into a physical movement.

Sageman concludes that a leaderless social movement is at the mercy of its participants. The main threat to the movement's existence is that its appeal is self-limiting. What appeals to one generation may not appeal to the next. Extremists and their messages must be demilitarized (deny young men the glory

of fighting uniformed soldiers of the sole remaining superpower) and reduced to the image of common criminals stripped of glory; extremism is about death and destruction, not fame. Counterextremism voices must encourage opportunity and reject violence. It is necessary to show young people they can address hopes, dreams, and grievances, without violence.

Remy Mauduit, noted above, recommended that the Department of Defense establish a permanent Islamic Information Center to assess, develop, disseminate, and coordinate information to the international Muslim public. Long term objectives would be to promote democracy, good governance, freedom, and human rights in the Muslim world. Short-range objectives would be letting the Muslim world know that the US continues to help it through repetitive broadcasting of the various humanitarian missions it organizes and runs. Themes to use and target audiences are:

- Supporting civil-society institutions
- Supporting both secularists and moderate Islamists
- Discrediting extremist ideology
- Delegitimizing individuals and positions associated with extremists by challenging their interpretation of Islam and promoting divisions among extremists by encouraging journalists to investigate issues of corruption, hypocrisy, and immorality in extremist and terrorist circles.
- Focusing on young people, Muslim minorities in the West, women, and the pious traditionalist populations, educating Muslims and non-Muslims alike on critical questions related to the compatibility between Islam and democracy.

Finally in February 2008, journalist Sharon Weinberger wrote that the gravest strategic lapse of the US government has been its anemic—if not self-destructive—effort to create and exploit divisions within and among jihadi groups, discredit their ideology, promote alternative Islamic voices, and isolate Islamic extremists. Weinberger seems to highlight the very themes that Maudit recommended. She states the US has failed to effectively counter portrayals of America as an aggressive, predatory force that poses a threat to Islam. The US government should stand up an independent agency to plan and orchestrate a coherent, national-level strategic communication strategy. All of this assumes, she notes, that the US government can compete with the global information market.

Frank Cilluffo, Chairman of the Homeland Security Institute's "Radicalization of the Internet" project, discussed his commission's findings in *IO Sphere* journal *[Summer 2007, p. 14.]* He noted that there are several ways to neuter terrorist use of the Web. His ideas were both more general, and yet in line with many recommendations that were to appear in 2008:

1. Understand the narrative and context of an extremist, why it resonates
2. Use all resources—no agency owns the mission
3. Defeat networks with networks, not a supercomputer
4. Use all elements of statecraft, not just the military
5. Remove terrorist masterminds
6. Offer opportunity to those who could be seduced by a terrorist message
7. Allow former jihadists to come forward and denounce terrorism
8. Substitute a new concept for the term *GWOT* (which to Cilluffo is as bad as the term *crusader* since it allows extremists to feel like warriors). Terminology matters
9. Require Islamic scholars to offer a counter dialogue
10. Find how to prevent someone from going from a sympathizer, to an activist, to indiscriminate violence. Discrediting extremism through religion is one option
11. Drive wedges between and among extremist and terrorist organizations (isolate planners from organizations, organizations from one another, and from society at large).

Also in 2007, Irving Lachow and Courtney Richardson, writing in *Joint Force Quarterly*, noted several US Government efforts to counter or delegitimize extremist use of the Internet. First, the State Department maintains a website in a number of languages devoted to countering false stories that appear in extremist sources, and countering disinformation that may end up in mainstream media. Second, military units conduct operational level influence operations for a long period of time. Lachow and Richardson discussed the utility of viewing the War of Ideas as equal in importance to military and law enforcement aspects of the fight. Finally, they recommended trying to find specific language with which to label Salafist extremists, such as *irhabists* (terrorist) conducting *hirabah* (unholy war) instead of *muhjahideen* conducting *jihad*; they recommended promoting the views of well-respected Muslim clerics who counter terrorist claims. Lachow and Richardson support attempts to undermine Internet-based terrorist influence operations and counters to a terrorist's operational use of the Net.

Conclusions

The consensus of experts appears to be that the use of secular or moderate religious figures or scholars have the most potential to effectively counter extremist Internet use. Such efforts could help to stifle some of the issues that extremists magnify in the Internet environment (death and destruction, Koranic verses of motivation). Getting secular or moderate figures online can help counter an insurgent's recruiting ability, and search for financial donations. Notably, several religious figures have recently been highlighted as contributing to this effort. Writing from prison in November 2007, Sayyid Imam al-Sharif published the book *On Rationalizations on Jihad in Egypt and the World*. Al-Sharif was a former aide to Al Qaeda second in command, Ayman al-Zawahiri. His counterextremism piece states it is religiously unlawful to use violence to overthrow Islamic governments. Another important figure, Sheikh Abd Al-Aziz bin Abdallah Aal Al-Sheikh, highest religious authority in Saudi Arabia, issued a October 2007 fatwah [Islamic legal pronouncement] prohibiting Saudi youth from engaging

in jihad abroad. Also in autumn 2007, Saudi cleric Sheikh Salman al-Awdah, wrote an open letter condemning Usama bin Laden. All of these individuals have had a strong impact on countering extremist recruitment and spread of their propaganda online.

Limiting the manner in which the Internet can shape opinions, through offering "other information or sources" that are deemed offensive to an insurgents cause, can certainly help the Coalition effort. Advanced societies have developed the virtual transnational communication network that insurgents can use at no or limited cost, and we must offset their efforts if the US hopes to succeed in the ongoing War of Ideas.

Today, terrorists are toying with the use of the virtual environment created by Linden Lab and known as *Second Life* (SL) [see "Exploring Second Life, Cory Ondrejka Interview," *IO Sphere* Fall 2007, p. 25]. A terrorist envisions SL as a means to communicate, launder money, or recruit individuals. There are measures in place to thwart this effort. First, Ken Driefach, Linden Lab's Deputy General Counsel, states that there are systems in place to monitor avatar activities and identify gaming behavior that may support a terrorist cause. Second, SL users can help counter terrorist use of the virtual gaming environment by monitoring information and communications exchanged among players and their activities. Finally, undercover operations could be initiated to provide information on groups with jihadist tendencies. Since the most often discussed solution to challenge insurgents is the use of clerics or imams to issue decrees, perhaps this option would also work in SL's 'virtual mosques?'

The *Second Life* case shows a small sample of other law enforcement issues. First, there are technological challenges. Insurgents skip from server to server, use anonymity as a friend, hide in chatrooms, move from one neutral computer source to another, and enter friendly systems at will to recruit or look for financial support. Second, Western nations must contend with extremist ideology that rejects anything other than their way of living and thinking.

To counter an extremist's use of the Internet, the Coalition needs to develop and execute the correct combination of constraining, monitoring, and deceiving extremists. Identifying which servers extremist groups use allows Coalition members to shut down those servers, and force (or even guide) an extremist to a new host. This constrains an extremist's activities, making it much more difficult to connect with their online user base and communicate new plans and activities. Monitoring allows one to get an inside look at how plans are developing. Insurgent's use of the Internet can also simply be shut down. Both of these options might involve deception, but the best use of deception is simply infiltrating a group and pretending to be someone you aren't. What about limiting content? If extremists are not provided material or video footage, they lose a major mobilizing factor. Simply making things more painful for extremists by disrupting communications should have a countering effect on their Internet activities.

Most significant of all, *an extremist* recommends ways to limit the ability of insurgents to communicate. Abu Yahaya al-Libi offered tips for better prosecuting the war of ideas against Al Qaeda. He noted that to defeat Al Qaeda, it was necessary to follow six steps:

- Focus on amplifying cases of ex-Jihadists who have willingly renounced the use of armed action and recanted their previously held ideological commitments
- Amplify Al Qaeda's mistakes, fabricate other mistakes, and ensure that any extremist group is used, not just Al Qaeda. Using other groups to serve propaganda purposes is known as "widening the circle"
- Government's prompting of mainstream Muslim clerics to issue fatwas (religious rulings) that incriminate the movement and their actions
- Strengthening and backing Islamic movements far removed from the fight, particularly those with a democratic approach
- Aggressively neutralizing or discrediting the guiding thinkers of the jihadist movement
- Spinning the minor disagreements among leaders or radical organizations as being major doctrinal and methodological disputes.

Al-Libi thus indicates the best way to influence an extremist movement is to 'strangle it by tying it up in knots.' It is unclear why he would develop such options for countering an insurgent's use of the Internet—bravado is one possibility. Another possibility is that he was merely regurgitating all that was written in 2007 about methods to counter insurgent Internet access and use.

Governments should force Al Qaeda into a series of compromising positions from a variety of angles so that it hangs itself over the long term. Hopefully the US Strategic Communication plan, and the organizations it will spawn in this new year, will be able to implement this strategy in an innovative manner.