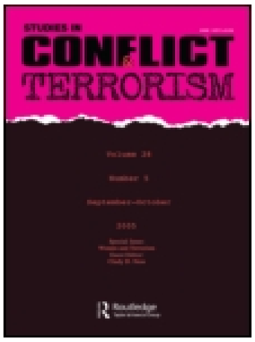

Routledge
Taylor & Francis Group

Studies in Conflict & Terrorism

ISSN: 1057-610X (Print) 1521-0731 (Online) Journal homepage: http://www.tandfonline.com/loi/uter20

The Vulnerabilities of Online Terrorism

Manuel R. Torres Soriano

To cite this article: Manuel R. Torres Soriano (2012) The Vulnerabilities of Online Terrorism, Studies in Conflict & Terrorism, 35:4, 263-277, DOI: 10.1080/1057610X.2012.656345

To link to this article: http://dx.doi.org/10.1080/1057610X.2012.656345

Published online: 19 Mar 2012.

Studies in Conflict & Terrorism, 35:263–277, 2012
Copyright © Taylor & Francis Group, LLC
ISSN: 1057-610X print / 1521-0731 online
DOI: 10.1080/1057610X.2012.656345

The Vulnerabilities of Online Terrorism

MANUEL R. TORRES SORIANO

Political Science Area
Pablo de Olavide University of Seville
Seville, Spain

Jihadist *terrorism has discovered in the Internet a valuable instrument to strengthen its activities. However, in using this technology the terrorists are exposed to new vulnerabilities. The Internet plays a leveling role: each new advantageous use it brings is accompanied by a new opportunity to weaken terrorist groups. The present article examines the main vulnerabilities of radical groups who have accorded the Internet a central role in their strategy, namely, less anonymity and security, a loss of content visibility, a major credibility problem, and an undermining of the legitimacy of the terrorist discourse as a consequence of their use of Web 2.0.*

Since its earliest days the Internet has given rise to mounting concern due to its potential use by individuals or groups for unlawful or criminal aims. Although it offers an inexhaustible array of resources for spreading knowledge, facilitating global intercommunication and lowering production costs, the Internet has also been the preferred tool for "shadier" sectors of society to increase their activities to undreamt-of limits.

This window of opportunity has not gone unnoticed by terrorist groups. In the early 1990s, even when the new technology was accessible only to a privileged few, a number of groups were already beginning to use it as a means of communication.[1] The technology has evolved in parallel to the evolution undergone by terrorism itself.

Much has been written on the motives[2] accounting for the transformation of the Internet into a powerful terrorism strategy asset: the facility, anonymity and low cost of access to the technology; little government control over the Internet; the possibility of using a multimedia environment, and so on. However, the truly revolutionary contribution has been the manner in which the technology has transformed the propaganda dimension of terrorist groups, turning their age-old dream of direct, intermediary-free communication with their potential "public" into a reality. For the first time, terrorists not only say what they want, but choose when and where to say it. Traditional media no longer represent an unavoidable filter. The terrorist message is transformed not so much to attract mass media attention but to heighten terrorists' powers of persuasion with respect to an audience that consumes the propaganda products directly and unaltered.

Received 26 May 2011; accepted 6 November 2011.

This article is part of a Research Project financed by the Spanish Ministry of Science and Innovation, "The Organizational Structure of International Terrorism: Implications for European Security (CSO2010-17849)," directed by Professor Javier Jordán, Department of Political Science, University of Granada, Spain.

Address correspondence to Manuel R. Torres Soriano, Political Science Area, Universidad Pablo de Olavide, Carretera de Utrera Km. 1, Sevilla, 41013 Spain. E-mail: mrtorsor@upo.es

However, the way this new mutation of an old threat has been put across to the general public has been characterized by dangerous simplifications. Anything relating to terrorist violence, particularly if associated with a technological component, is easily adapted to the mindsets and the preferences for sensationalism and hype of certain media. The average spectator is overwhelmed by a series of messages that consolidate many of the clichés projected by films and fiction series dealing with terrorism.

Although the media correctly identifies the Internet as a veritable turning point in the general history of terrorism, its treatment of the subject has tended to be almost always one-dimensional, with constant emphasis on how terrorist groups have benefited and scant attention devoted to their new weaknesses. Like all complex phenomena, the Internet is essentially dual in nature. The new opportunities available to terrorists thanks to cyberspace are balanced by new vulnerabilities. In this regard, the Internet has simultaneously become an ally as well as an enemy of terrorist organizations.

The aim of this article is to outline what is considered to be the main vulnerabilities to which terrorist groups who accord a key role to the Internet in their strategy are exposed. To that end the article will focus attention on the clearest exponent of the new online terrorism: Al Qaeda and the other organizations, networks, and individuals that gravitate around it.

A Watered Down Anonymity

Cyberspace is the safest of the public communication channels used thus far by terrorist organizations. The considerable anonymity afforded by the technology has allowed thousands to enter into contact with terrorist subcultures without endangering their own safety in any way. This confidentiality is not, however, total. People often attribute a range of characteristics to the Internet that bear little resemblance to its true nature. In fact, a substantial portion of these perceptions stem from experience as people living in democratic countries that respect the privacy of their citizens. However, the anonymity of the network of networks fades somewhat if one bears in mind the experience of those living under dictatorial regimes that are characterized by their disregard for secrecy of communications and suffer the most serious material underdevelopment. In these countries (almost all of them in the Muslim-Arab world) the fact that very few are in a position to enjoy an individual Internet connection facilitates the work of law enforcement agencies enormously as regards identifying Internet users. The anonymity of a network can be said to be directly proportional to the number of its members. In the majority of cases, obtaining a connection depends on arbitrary concessions by the authorities, with the political powers weighing up a priori the intentions of the applicant.

For security reasons, many potential consumers of Internet-based terrorism messages try and avoid browsing such pages from home. A public computer or an Internet café apparently affords greater anonymity. In Islamic countries, however, it is normal for the authorities, for reasons of political and social control, to impose restrictions on the type of service provided by such establishments. For example, terminals must be visible to the public, access to certain sites is blocked, client identities must be recorded beforehand, and so on. One of the most common restrictions is to disable browser options that allow the user to delete the history of sites visited. Consequently, the computer stores a detailed record of all types of use made by every user. Online terrorism addicts are forced to operate in a public environment that harbors a latent threat that their browsing has been monitored by infiltrated police officers or informers or that the security forces may be tipped off by other users, including the owners of the premises. "Cyber *Jihadists*" are fatally dependent on public computers. They need them even though they are aware that every connection entails a dangerous exposure to discovery.

On 13 September 2010 a senior member of one forum in Arabic posted guidance for colleagues on how to avoid detection. With regard to Internet cafés, "especially those with an Islamic look. Be careful!" he advises users not only to stay for just a short time but to use different cafés as far away from home as possible. "These cafes are under tight surveillance because the tyrant security agencies are fully aware of all the IP addresses of every Internet café."

Some of his recommendations are based on a total mistrust of the forum administrators, either because they may conceal the enemy or the servers can be hacked into and information stolen. Accordingly, he advises his colleagues never to access such sites from home or open from home an e-mail account used for identification purposes on the forums. He also recommends using different user names and passwords for different websites and cautions against downloading any program offered via the sites, and so on.

The real danger of detection has led Jihadists to shun the forums' socializing function and the possibilities they can offer to create trustworthy networks: "If you were one of those who like to meet people and have friends, be sure that the jihadist websites are not the appropriate place to do it!"

This predicament is a major constraint on the communication strategy of *Jihadist* terrorism, which is directed largely at people living in Muslim-majority countries. For this reason the groups have had to persist with their efforts to attract the attention of the traditional media (television for the most part) due its mass audience and the fact that a TV screen continues to be more "anonymous" than a PC.

Technology Flip-Side

The fascination that the new information technologies have triggered among *Jihadists* has been accompanied by a contradictory sentiment of fear. Computer viruses, trojans, spyware, and so on, can also be used for counterterrorism ends. One of the tools most feared by *Jihadists* are so-called sniffers: small, hard-to-detect programs that can be inserted covertly via the Internet on any computer and used by the controller to eavesdrop on all data traffic on the Web and reveal the identity and habits of the victim.

The existence of these sophisticated computer resources and the assumption by the *Jihadists* that they are in the hands of an enemy such as the United States, which is not just the world's biggest military and economic power but also the most important in terms of technological innovation, has generated genuine paranoia among online terrorism regulars. *Jihadist* websites devote increasingly more space to advice on the security measures to be adopted when using the sites, downloading files, using e-mail accounts, participating in forums, and so on. The sites constantly reflect speculation on how the enemy might be using this "flip-side" of the technology to curb the *Jihadist* movement. However, since they tend to be unsophisticated and are voiced openly, and are therefore accessible by the infiltrating agencies, the recommendations are not sufficient to immunize Internet activists from infiltration attempts. Intelligence services have the necessary information to know how their targets will try and evade the trap set for them. The recommendations are rendered totally counterproductive on occasions since they indicate how a cyberspace *Jihadist* should behave and therefore make him recognizable.

Every time an arrest is made or a terrorist plot is uncovered radical forums are inundated with speculation as to the causes leading to the arrests. One possibility constantly raised is technological infiltration but it is a sterile recurring lament given that the site users have no way of confirming their theories. Structuring terrorism on the Internet can serve to pool and give cohesion to the endeavors of thousands of people scattered around the world who are not in direct contact or communication with each other. Yet these very characteristics rule out the advantages that come with hierarchically structured organizations, including a detailed knowledge of the vulnerabilities of certain components, knowledge that might be of help with a view to remedial action to prevent a repeat occurrence. When the security forces arrest one of these online terrorists, his voice is silenced among the cybercommunity and its members are deprived of the information that could lead it to identify the source of its weakness. The conclusions found on these sites are based on incomplete information, much of it obtained from operational details divulged by law enforcement agencies, who are thus in a position to include misinformation aimed at encouraging the terrorists to repeat their mistakes.

A clear example of how fear of technological infiltration weakens and incites confrontation among the Internet *Jihadist* community can be seen in the bitter dispute[3] that arose between two of the most important *Jihadist* Web forums. In mid-2006 the influential *Tajdeed* forum openly accused its brother forum *al-Hesbah* of being responsible for the arrest of 40 *mujahideen* in Saudi Arabia. It believed that the website had been openly penetrated by Saudi intelligence, thus enabling the latter to detain the perpetrators of the attack on the Abqaiq refinery (25 February 2006) just six hours after they posted a message on the forum claiming responsibility for the attack. Several other elements of suspicion pointed to *al-Hesbah,* for example, the clear majority of Jordanians (whose intelligence services cooperate closely with the United States) among the forum administrators and the fact that new forum members were admitted only after supplying genuine information on their country of origin. Moreover, the site did not permit software tools that helped conceal the site user's geographical origin.[4] Participants in the *Tajdeed* forum have also complained of infiltration of another important *Jihadist* propaganda vehicle, the *Global Islamic Media Front* (GIMF).[5] They allege that the platform put out a video entitled *Dima' Lan Tadi'* ("Blood that will not be lost") with the audiovisual testament of Fahd bin Faraj al-Juweir, one of the leaders of Al Qaeda in Saudi Arabia, who was shot dead by police three days after the Abqaiq refinery attack. It was alleged that the video had fallen into police hands following a raid over a year earlier. Indeed, the Saudi authorities had distributed in February a photograph taken from the video in calling for public cooperation to arrest the terrorist and warning of his plans for a suicide attack. According to the *Jihadist* forum, the video was posted by Saudi agents to raise the credibility of the infiltrated GIMF and persuade other terrorist organizations to use it for their communiqués, which would inevitably lead to further arrests.

Due to the fear of alleged infiltration, apparently innocuous events take on conspiratorial tones, helping set in motion chain reactions that end up weakening the terrorist presence on the Internet.

An interesting example of this paranoiac behavior can be seen in the events surrounding the distribution of *Inspire*, the first *Jihadist* magazine in English, in the summer of 2010. What was supposed to be one of the main propaganda initiatives of Al Qaeda in the Arabian Peninsula descended into cyber-panic when the *Jihadists* realized that the PDF file containing the magazine had become corrupted and only the first few pages could be viewed. Soon after, the moderators of the main *Jihadist* forum at the time, *Al-Falloja*, posted messages warning that the *Inspire* file was infected and had been removed from the forum. Almost immediately, further messages from the moderators alerted members that the site had been compromised and users were urged to delete their private messages and change their passwords.[6] Immediately also some users began to write to say that they were prevented from carrying out the instructions because someone had blocked their access to the account control tools. Panic set in and the site crashed shortly afterward and was no longer available on the Internet.

Other forums tried to preempt the alleged attack by switching off their sites. Days later, *Al-Falloja* reappeared with just one message by way of content: a brief communiqué outlining the events that had prompted its closure. The site became operational once again on 9 July but something had happened in the meantime. *Al Falloja* had been, until then, one of only two sites to host propaganda from *Al-Fajr*, the official media platform for communiqués by Al Qaeda and its affiliates. However, it suddenly stopped providing such materials.[7] The forum's credibility had been fatally damaged and *Al-Fajr*, having lost faith in the website, ceased supplying it with videos and written documents from *Jihadist* groups and leaders. The consequences were inevitable: a month later, a message from the administrators appeared on the forum announcing it was closing within a week but offering nothing by way of explanation. A year later, it was disclosed in the media[8] that the panic in the *Jihadist* Internet infrastructure had been caused by a cyberattack by Britain's MI6 intelligence service, whose officers, prior to the release of the original magazine on the Web, replaced some of its pages with garbled computer code from a Web page of recipes for "The Best Cupcakes in America." The manipulation, dubbed "Operation Cupcake" by the media, featured a touch of humor given that among the pages replaced was an article by "The AQ Chef" entitled "Make a bomb in the Kitchen of your Mom," which offered instructions for building an explosive device using household materials and kitchen substances such as sugar.

Consumers of materials of this type are disconcerted by the glaring lack of information surrounding some of the main incidents concerning the *Jihadist* presence on Internet.[9] Their only resource is to spread a near-infirm mistrust of anything originating in cyberspace: antivirus software, navigation tools, commercial e-mail accounts, and so on. Absolutely everything is suspected of concealing a trap. For example, a *Jihadist* site warned its followers "to be careful with Google."[10] The message alleged that Google's new free toolbar concealed a range of functions that allowed the company access to detailed knowledge of everything stored on the computers on which the toolbar is installed. The terrorists know that the main utilities and some of the resources that make Internet so attractive are owned by American firms and they have no doubts as to the willingness of these firms to cooperate with their government. Consequently, a whole range of resources essential for full use of the Internet are potentially hostile, albeit indispensable.

Efforts to come up with software capable of eliminating threats of this type appear to have been unproductive. The *Jihadists* created and distributed on the Internet two versions of an applications package called Mujahideen Secrets, which aimed to give cyber-*Jihadists* a trustworthy tool to encrypt their communications, erase digital traces of their browsing, and meet all other needs to guarantee their anonymity and security. However, even the use of this program has been hit by the spiral of mistrust that characterizes the *Jihadist* presence on the Internet. In March 2011 the GIMF published a message[11] indicating that copies of the program had been manipulated and offering a set of new safe links. Thus, even something that was created to safeguard the anonymity of the *mujahideen* has become a source of fresh fears.

Diminishing Visibility

A widely held belief with respect to the terrorist presence on the Internet is that it is impossible to try and block the existence in cyberspace of webs that serve the aims of such groups. The argument goes that the very nature of the network of networks makes it unthinkable to silence their discourse through hacking actions or cooperation from the infinite number of Web hosting companies that accommodate such sites on their servers. However, this belief, although true, can be qualified to a certain extent. It would be futile to attempt to eradicate all such sites since this would require tasking the same number of people to attacking the sites as the number willing to set up new ones or resurrect ones already targeted. The sheer numbers would be unworkable. The same is not true, however, if the objective is to bring down a specific site, such as one administered by members of a terrorist organization as their official platform. In these cases, intelligence agencies (and even spontaneous collaborators) can focus on a very small number of targets and hence silencing a specific "voice" becomes feasible. This strategy is appropriate to the pyramid structure of the *Jihadist* presence on the Internet. Although several thousand websites support and promote the terrorist discourse, not all are of the same importance or produce the same impact. The pyramid is headed by a small number of sites that are differentiated from the rest in that they are the only ones to directly receive materials prepared by terrorist groups. On these one can find, in the form of exclusives, ideological diatribes, interviews, and audio and video recordings of recent acts of violence. The other sites simply repeat, amplify and re-elaborate the new content disseminated by the *Jihadists* who carry out the *Jihad* in person.

Maintaining a stable Internet presence capable of reaching all potentially interested individuals has not been easy for *Jihadist* groups. Initially, many organizations set up their own sites to post their communiqués, operational videos, and materials of interest.[12] However, the strategy was soon discarded due to its many drawbacks.[13]

Official sites such as that of Al Qaeda (alneda.com) came under incessant attack in the aftermath of 11 September 2001 and were forced to migrate constantly across the Internet disguised under various hosts and domains until they disappeared definitively.[14] *Jihadist* networks have gradually abandoned their designs of maintaining an official site due to the massive time and work required, which could turn out to be fruitless given that designating a site as an official mouthpiece would automatically see it targeted by an infinite number of attacks from the four corners of the planet. An alternative strategy has been to evolve toward a much more horizontal and diffuse Internet presence based on networking by a broad range of volunteers. This new phase has been spearheaded by Internet forums,[15] spaces that offer a host of useful functions for *Jihadist* networks but that, above all, have become excellent tools for disseminating propaganda.

Events of recent years support the view that the "shelf-life" of a website is inversely proportional to the importance it is accorded in the *Jihadist* universe. According to Aaron Weisburd, the creator of *Internet Haganah*, an organization dedicated to monitoring the Jihadist presence in cyberspace, 80 percent of the main websites to emerge between 2002 and 2004 have disappeared because they have been unable to withstand the continuous harassment by security agencies, private groups, and hackers.[16]

The terrorist presence on the Internet is increasingly unstable, thus hampering the groups' propaganda strategy. Al Qaeda Central, for instance, has sought for years to make the anniversary of the 9/11 attacks a date on which world public opinion should focus on the group's discourse. To that end it has released messages in which the anniversary is made to coincide with a propaganda "exclusive": video testaments from the plane hijackers; footage showing how the attacks were prepared; a rare video appearance by its elusive leader, Osama bin Laden. As a result, news coverage of the tributes to and memories of the victims would inevitably be accompanied by the latest news exclusive on those responsible for the macro-attack. To heighten expectations and enhance the media repercussions of the messages, the group even began to add, in the days leading up to the anniversary, advertising banners with pictures on *Jihadist* forums giving advance notice of the forthcoming videos.

To mark the seventh anniversary of the 9/11 attacks the group announced the posting of a video entitled "Results of 7 Years of the Crusades," featuring words from senior figureheads such as Ayman al-Zawahiri, Mustafa Abu al-Yazid, and Abu Yahya al-Liby. However, on 10 September, without explanation of any kind, the main forums on which the video was supposed to appear suddenly went offline, setting off speculation as to the origin of the blackout. Was it a cyberattack? A preventive measure? Who was responsible? A week passed before the *Jihadist* websites were restored and offered the usual links to sites from which the video could be downloaded. However, something unforeseen occurred again. Forum users could download the video but could not view it because a password was needed to unzip the contents and the password provided by the forums did not work. Again all kinds of speculation were triggered on the forums as to this unprecedented occurrence: Was it human error? Sabotage? The frustration grew constantly because it took the webmasters almost a full day to provide the correct password, but without offering any explanation to clarify the incident.[17] In September 2009 and 2010 delays again hit the dissemination of the Al Qaeda anniversary video after the main forums were sabotaged and put out of action for several days.[18]

Occasionally, steps taken by the websites themselves generate a loss of visibility and influence. Some administrators choose to protect their Web content by making it available only to users who identify themselves with a password. Similarly, several *Jihadist* forums have decided at some stage to restrict access to their content to registered users and do not allow new members. This strategy was used by the administrators of some leading propaganda distribution forums in order to curb the growing number of critical comments from users. The *al-Shmukh* forum[19] did precisely this after the attack carried out on a Christian church in Alexandria (Egypt) during the 2011 New Year celebrations. Some Web users belonging to the Coptic minority in Egypt began to post hostile comments on the forum in response to posts from other users in which information was given on the location of other Coptic Christian targets.

When this occurs terrorist websites sacrifice the prospect of a wider audience in exchange for guaranteed site content coherence. This drastic response in turn generates controversy among forum users. On one side are those who challenge the practice because it impedes the spread of the discourse among the Muslim community.[20] Restricting a forum through a password makes it inaccessible to commercial search engines that could direct potential users toward the forum's content. The registered forum users become a small group operating purely on self-feedback and increasingly distanced from the *ummah* (the community formed by all Muslims). On the other side are those who consider that if restrictions are not imposed on forum participation there is a risk that the purity of the *Jihadist* message might deteriorate to the benefit of the masses.

The decline in the *Jihadist* presence on the Internet has become more accentuated with the assumption by the radicals that the Internet is an increasingly hostile territory. One example of this attitude was the announcement, in September 2010, of the creation of a new forum called *Shabakat Al-Nur Al-Islamiya.*[21] Unlike its predecessors, this radical forum only accepted as members users with a proven cyber-*Jihadist* track record, using as a criterion that they had to have written 150 quality posts on the *al-Tahadi* forum, where the setting up of the new platform was announced. The launch of a new forum designed to bring together the elite of radical Web users generated a bitter dispute[22] among *al-Tahadi* users. Some began to question the credibility of the proposed forum and asked who had authorized the setting up of a new *Jihadist* platform on the Internet. The growing discontent among users forced the administrators of *al-Tahadi* to do a U-turn and announce officially that the initiative had been abandoned.

The above episode illustrates the contradictory tension that exists in the *Jihadist* Internet universe between those players who seek greater security and ideological homogeneity, even at the risk of creating increasingly closed and opaque groups, and those who fear that the *Jihadist* movement will become inward-looking and, eventually, irrelevant in the immensity of the cyberspace community.

Although they afford greater anonymity and security for users, some of the practices adopted, such as channelling most interaction via private chats on forums or arranging to conduct conversations using VoIP technology, have resulted in a loss of visibility for the radicals' message on the Internet. The *Jihadist* presence in cyberspace is increasingly a concealed area with diminished capacity to attract Web users lacking the contacts and connections needed to get round the wall of mistrust erected by the radicals to protect themselves.

The step-up from virtual activism to interaction with others in the "physical" world is increasingly hampered by the plethora of stories and rumors concerning enemy traps that have served to paralyze some of the most committed cyber-*Jihadists*. The possibility that the user with whom conversation is taking place is actually a law enforcement officer posing as a *mujahideen* wanting to travel to a *Jihad* "hot spot" has even led some users to draw up a check list to help detect whether "your Jihad recruiter is an FBI agent."[23]

The Credibility Battle

The first step before an Internet user enters the *Jihadist* cybercommunity is for the latter to decide whether or not to trust a range of content prepared and disseminated by individuals whose identity, qualifications, and ultimate goals it does not know. With the exception of a very small group of people who know some of the webmasters personally, the great mass of followers of these spaces need to trust their instinct when making their choice. Although there are some "motifs"[24] that identify genuine *Jihadist* sites the job is not always an easy one given that all these elements can be imitated readily.

Following the 9/11 attacks the Internet witnessed the mass arrival of individuals keen to use cyberspace for their contribution to the global *Jihad* against the United States and its allies. They not only set up spaces to amplify the terrorist message but also created a series of names that were used for a "psychological war" on Western societies. These are the so-called phantom groups: fictitious organizations that have capitalized on the anonymity afforded by cyberspace for their own propaganda actions. The best-known example of these "screens" are the so-called Abu Hafs Al Masri Brigades, who issued a series of communiqués that achieved significant impact in world public opinion. The Brigades have a long track record of falsely claiming responsibility for attacks carried out by others and even for incidents totally unrelated to terrorist violence, examples being the London bomb attacks of 7 July 2005 or the fortuitous power blackout that hit northeastern parts of the United States in August 2003.[25]

The messages have achieved enormous success in terms of media impact. Astute selection of the release dates for the Brigades's statements has ensured that on occasions the effect of the threats and claims has surpassed the physical impact of the attack referred to.

The major repercussions in the West of all terrorism-related news have spurred the communications activities of these phantoms groups. One of their main activities has been an intensive threat campaign including statements on new targets, warnings of attacks of apocalyptic dimensions and advice to Muslims to avoid certain locations given the impending disaster.

> Europeans, you have just 15 days to accept the truce offered by Bin Laden, otherwise you and you alone will be entirely responsible. ... Those who can return to Islamic countries should do so, those who cannot should be careful and stock up with enough food and money for a month or more.[26]

The media impact of these messages has encouraged those sympathetic to *Jihadist* terrorism to follow suit and new names have proliferated, including the Mohammed Atta Brigades, Ansar Al Zawahiri, Al Islambouli Brigades, and so on. Other cyber-*Jihadists* have opted to make use of "consolidated brand names" and, despite not having any contacts with the leaders of the Brigades, have issued new threats in their name, which has led to the ludicrous situation whereby *Abu Hafs* has been forced to issue its own communiqués denying the veracity of threats made in its name.

Communiqués from these groups contribute significantly to the general *Jihadist* terrorism strategy because they raise the stress levels in the societies targeted by the threats and hamper the work of security and intelligence agencies, who constantly have to assess the credibility of, and the response to, the incessant threats issued using these names. However, the actions of such "phantom groups" have had disruptive repercussions on the communications strategy of "real" terrorists. Both Al Qaeda and its affiliates painstakingly plan the propaganda exploitation of their terrorist actions and carefully calculate the timing of messages. The emergence of these alternative contents can occasionally hamper these communication strategies, upsetting the timings aimed for by the terrorists and causing confusion among audiences. As a result, *Jihadist* groups have been forced to modify the channels used to disseminate their messages and caution their "public" to consider as legitimate only those communiqués posted by the group's official mouthpiece or for which advance notice has been given. The actions of the aforementioned "brigades" have resulted in *Jihadist* webmasters only accepting as valid the messages received from a trusted e-mail address.

However, the main vulnerability of Web-based *Jihadist* propaganda stems from the "information operations" launched by intelligence services keen to exploit the credibility battle waged on the Internet. An interesting example of such operations was the dissemination of a fake issue of the "Voice of Jihad," the flagship online publication of Al Qaeda in Saudi Arabia. Readers of the publication encountered simultaneously on the Web two completely different Issue No. 14s, a situation that triggered major confusion and forced the authors to change the distribution system, alerting readers that the only legitimate source of the magazine would be a specific Internet domain, details of which would be revealed in advance via the *Global Islamic Media Group* mailing list.[27]

The death of Osama bin Laden in May 2011 also afforded a window of opportunity to use the Internet to create confusion among the radicals. An interesting example was the fake "official" announcement on the Tahadi forum that bin Laden's own son Hamza was to succeed him as Al Qaeda leader. The communiqué and its advertising banner were promptly removed by the site administrators and participating users were expelled from the forum. However, once again, it remained unclear whether the accounts of users who had clearance to post materials had been hacked or whether the website had been taken over by "enemies." In any event, certain followers inevitably began to query the reliability of this virtual platform: "the Tahadi of today is not the same Tahadi as it was in 2009."[28]

Individual disinformation activities have also been undertaken in chat rooms by members of the international intelligence community, with fluent speakers and writers of Arabic, Farsi, Urdu, Pashto, and other languages painstakingly creating false identities and interacting online with site users to gain their trust and subsequently feed them information designed to cause confusion or confrontation on their networks.[29]

The credibility of the *Jihadist* message on the Internet is also compromised by the existence of "entrapment" websites that offer content resembling the Al Qaeda message to gain the trust of the *Jihadist* audience and then erode the virtual community from within. Given that infiltration of established *Jihadist* forums is very difficult due to the existence of a series of preestablished symbols, codes, and concepts, it is more feasible for intelligence agencies to set up so-called honey pots to reverse the process and entice the *Jihadists* themselves into the open. Although no agency has openly admitted participating in such information operations, in March 2010 the *Washington Post*[30] reported on the first implicit acknowledgment of the use of techniques of this nature. According to the paper, in 2008 an incident that reflected the lack of coordination and the conflict between U.S. agencies served to illustrate the credibility problem Internet radicals have to contend with. According to the report, some U.S. military leaders were convinced that a *Jihadist* forum[31] administered covertly by the CIA and Saudi intelligence was being used by radicals to coordinate attacks against American soldiers in Iraq. The Pentagon was convinced the forum had to be shut down because of the danger it posed for troops. However, those running the operation defended its crucial worth as a mechanism for gathering intelligence on terrorist networks and even as an instrument to foil terrorist plots before they materialized. Despite opposition from those in charge of this intelligence-gathering operation, the Pentagon forced the site to close by launching a cyberattack that crippled it.

Dutch intelligence (AIVD) carried out a similar operation, administering a false *Jihadist* website that enabled officers not only to access the details of users and monitor communications sent via the site but also to infect with spyware the computers of radicals who downloaded material from it.[32]

The use of the Internet has become increasingly shrouded in uncertainty for terrorists because of the ever-present danger of being snared by the "spider's web" weaved by the enemy. Fake sites are a constant source of concern for the *Jihadist* cybercommunity, which witnesses heated debates on the authenticity or otherwise of certain sites. The climate of permanent suspicion[33] is not only nurtured by the speculations of grass-roots users but even by instructions issued by the leaders of the media *Jihad*. For example, Abu al-Aina'a al-Khorasani, one of the administrators of the *al-Falluja* forum, the official recipient of Taliban propaganda materials, warned members that the "group's main site and the site of its online journal Al-Sumud, have been the subject of an 'infiltration operation.'"[34] According to this cyber-*Jihadist*, nobody should access the website of the Islamic Emirate of Afghanistan or open any of its links until they receive confirmation from "your brothers."

The Perils of Web 2.0

Jihadist groups have shown themselves to be highly innovative in terms of capitalizing on the succession of technical advances made by the Internet. They have, for example, adapted their Internet presence to the Web 2.0 philosophy. Users are increasingly abandoning the role of passive consumers of materials accessible on the Internet (Web 1.0) and are increasingly engaging with the new virtual reality, generating their own content.

Jihadist organizations have made great efforts to convey the idea that the *mujahideen* are in permanent communication and contact with Muslim society. On 16 December 2007, for example, the media branch of Al Qaeda, *Al Sahab*, and the *Al-Fajr Media Center*, a virtual platform for distributing *Jihadist* propaganda, announced on the Internet a joint initiative under the name of "Open Meeting with Al Zawahiri." Journalists and *Jihad* supporters were invited to submit questions or doubts to the terrorist leader using the main *Jihadist* forums. Three months later, the then Al Qaeda Number 2 personally answered a selection of questions in an audio recording lasting almost two hours, which was accompanied by a transcript of the contents in Arabic and English.

Initiatives of this kind have afforded *Jihadist* groups considerable propaganda mileage and allowed them to cultivate an image of proximity to the Muslim masses they purport to defend. The success of the interactive contact with radical forum users can be gauged from the 1888 questions submitted from all corners of the world via the three main *Jihadist* forums of the day.[35]

However, Al Qaeda use of Web 2.0 has brought some counterproductive consequences for the group. To begin with, in selecting questions for replies, al- Zawahiri did not choose the most common topics raised by Web users but rather ones that allowed him to reiterate the classical Al Qaeda propaganda themes, along with other issues of particular interest to the leadership at that time. For example, he ignored a large number of questions on the internal workings of the organization but devoted considerable time to answering the few asked about relations between Al Qaeda and certain Islamic movements such as the Muslim Brothers.

The potential problems of such "openness" for *Jihadist* ideologists have led them to restrict the visibility of user contributions. In the summer of 2009, for instance, the *Al Shumukh* radical forum held an "open forum"[36] with the renowned Jordan-based cleric, Abu Muhammad Al Maqdisi. The rules of participation in the virtual meting stipulated, however, that the questions would only be readable by the radical sheikh, a decision that was designed to prevent users from knowing not just the questions asked by others but also that had been selected by Al Maqdisi.

Jihadist groups seeking an intensive Internet presence must contend with the paradox that interaction with Web users allows them to attain their goals by creating a sense of virtual community, consisting of individuals who share and mutually reinforce their radical beliefs, but at the same time the same instruments that nurture the cybercommunity also open the door to dissident actions or critical voices who can gradually erode the ideological orthodoxy of the terrorist movement. Thus, one participant in the *Al-Falloja* forum asked the following accusatory question of the site administrators:

> Why are there no Palestinians in the leadership of the Global Jihad? Why are the Mujahideen in Iraq killing the local security forces and not focusing on American soldiers? Also, why are Al-Qaeda activists killing Algerian soldiers and not fighting in Iraq or Somalia? Why does Al-Qaeda not attack in Israeli territory or Israeli embassies worldwide?. . .[37]

The emerging criticism and even ridiculing of *Jihadist* propaganda is even more marked on other Internet spaces over which the terrorist organizations have little or no control. One of the clearest examples is the popular YouTube video-sharing site. The presence on the site of many recordings by terrorist organizations or their followers has triggered considerable alarm among Western public opinion,[38] not least because a space on which millions of people watch and share harmless content is being used also for calls to violence and images of murders and kidnappings. However, one aspect that has gone unnoticed is that, due to its philosophy, YouTube not only lets any user upload radical content but also allows anyone to comment on the video. Thus, videos of bin Laden and his followers have not just been replicated, viewed, and celebrated thousands of times but have been criticized and ridiculed to the same degree.[39] The YouTube presence of the *Jihadists*, although raising the visibility of their message, has proven an excellent means of debunking and undermining the solemnity of the radical message, which is rejected by a multitude of Muslim and non-Muslim Internet users. In this regard, one could argue that the more *Jihadist* terrorism commits to Web 2.0 the more it exposes its discourse to challenge.

By way of example, in December 2009 Al Qaeda distributed on the Internet *Jihadist* forums a new video in English entitled "The mujahideen don't target Muslims" and featuring one of its members, U.S. citizen Adam Gadahn, alias "Azzam the American."[40] The video is an attempt to exonerate *Jihadist* groups from blame for attacks on Muslim civilians in mosques, markets, and other busy places in Iraq, Afghanistan, and Pakistan. According to this Al Qaeda spokesman, the accusations were fabricated by media acting as "weapons of propaganda in the pockets of the crusaders and their puppet governments and armies allied with them." Addressing Muslims, he says "your true friends and protectors are the Muslim mujahideen, who have risen up to defend you and your religion from these criminals."

The video was posted on YouTube for the most diverse reasons by scores of users, ranging from Al Qaeda sympathizers keen to increase the dissemination of this propaganda production to others who hoped to illustrate through the video, using as their argument the Jewish origins of Azzam the American, their accusations that Israeli intelligence services are behind world terrorism. However, the most intriguing aspect is that the praise voiced by some for the truth contained in this Al Qaeda communication is forced to coexist with indignant reaction from Muslim and non-Muslim users alike. One of the copies of the video[41] merited the following response from a user who goes by the name *acerb45666555*:

> What? Al Qaeda-Taliban do not kill Muslims? Yes, you do. You kill Sufis, you kill Muslims who want to bring some parts of the West into their lives, you kill Muslim children in schools in Afghanistan, you rob and kill the medical personnel who help your own tribes . . . .

Conclusions

Terrorists have discovered in the Internet a valuable instrument for strengthening their most important activities. The technology has not only given these groups greater scope and made them more dangerous but has also allowed them to deploy new social mobilization strategies.[42] However, the nature of the Internet is dual. Terrorists are inevitably exposed to new vulnerabilities when using such technology. The Web acts as a leveller: each new advantage for the terrorists is accompanied by a new opportunity to weaken such groups.

Although the commonly held view is that, on balance, the terrorists clearly stand to gain from Internet use, the fact is that the Internet is a neutral territory. It is the skill of those who use the technology that determines its character. All new opportunities for terrorists in cyberspace have their respective nemesis. Some of the responses are obvious, others emerge spontaneously, and a third group requires considerable creativity. In fact, the counterterrorist response on the Internet has become increasingly sophisticated and effective of late. It has taken security and intelligence agencies several years to develop the capabilities required for specific cyberspace actions that have eroded the trust deposited by *Jihadist* networks in the Internet. Infiltration, sabotage, and monitoring actions of this kind have helped undermine the feeling of impunity enjoyed by radicals in their cyberspace activities. Networks operating on the Internet are beginning to encounter serious difficulties in their efforts to retain visibility and operate effectively.

There is no reason to believe that terrorists have found in the Internet a refuge that they cannot be deprived of. Just as in a "physical" environment, terrorists can be contained in cyberspace. However, effective action in this new terrain requires the same flexibility and innovation demonstrated by the *Jihadists*. The key to attaining this objective is to engage civil society in the fight against the terrorist presence on the Internet. The model to be imitated is that applied to the battle against Internet child pornography, through the creation of formalized channels for Web users to send information and denunciations to the competent authorities. Participation by civil society in curbing the terrorist presence on the Internet would act as a multiplier for the efforts of law enforcement agencies, whose intelligence-gathering capabilities and ability to get to grips with the wide-ranging terrorist presence on the Internet would be multiplied at no cost.

Notes

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

2. Daniel Kimmage, *The Al-Qaeda Media Nexus: The Virtual Network Behind the Global Message* (Washington, DC: RFE/RL Special Report, 2008); Evan F. Kohlmann, "Al-Qa'ida's 'MySpace': Terrorist Recruitment on the Internet," *CTC Sentinel* 1(2) (2008), pp. 8–10; Maura Conway, "Terrorism and the Internet: New Media, New Threat?," *Parliamentary Affairs* 59(2) (2006), pp. 283–298; Jarret M. Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," *The Fletcher Forum of World Affairs* 30(2) (2006), pp. 149–164; Javier Jordán and Manuel R. Torres, "Internet y actividades terroristas: el caso del 11-M," *El Profesional de la Información* 16(2) (2007), pp. 123–130.

3. Gabriel Weimann, "Virtual Disputes: The Use of the Internet for Terrorist Debates," *Studies in Conflict & Terrorism* 29(7) (2006), pp. 623–639.

4. Stephen Ulph, "Intelligence War Breaks out on the Jihadi Forums," *Terrorism Focus* 3(14) (2006).

5. Stephen Ulph, "Fears of Intelligence Penetration of the GIMF," *Terrorism Focus* 3(16) (2006).

6. MEMRI, "Jihad & Terrorism Threat Monitor Weekly Digest No. 37," *Special Dispatch* 3086 (July 2010) (by subscription).

7. D. Hazan, "Tension, Suspicion Among Jihadi Websites Following Infiltration, Collapse of Several Sites," *MEMRI Jihad and Terrorism Threat Monitor, Inquiry & Analysis* 625 (July 2010) (by subscription).

8. Duncan Gardham, "MI6 Attacks al-Qaeda in 'Operation Cupcake,"' *The Telegraph* 2 June 2011.

9. On 13 August a user with the pen name Irhabi li-Nusrat-al-Din wrote on the same forum: "Here is another shock, a new shock that jolted us recently in an extremely surprising way. The jihadist forums that were to shut down had closed abruptly for days before a permanent closure was declared. Sometimes, there were declared reasons, but other times the shutdowns had unknown reasons- (. . .) This announcement created an unanswered question, resonating: O my God! What happened?"

10. Yuki Noguchi and Sara Kehaulani Goo, "Terrorists' Web Chatter Shows Concern About Internet Privacy," *The Washington Post* 13 April 2006.

11. "Global Islamic Media Front announcement," Shamik Forum. Available at http://shamikh1.net/vb/showthread.php?t=96252 (in Arabic) (accessed 20 March 2011).

12. Evan F. Kohlmann, "The Real Online Terrorist Threat," *Foreign Affairs* 85(5) (2006), pp. 115–124.

13. Manuel R. Torres Soriano, "Maintaining the Message: How Jihadists Have Adapted to Web Disruptions," *CTC Sentinel* 2(11) (2009), pp. 22–24.

[14] Brynjar Lia, "Al-Qaeda Online: Understanding Jihadist Internet Infrastructure," *Jane's Intelligence Review*, 1 January 2006.

[15] Hanna Rogan, "Al-Qaeda's Online Media Strategies: From *Abu Reuter* to *Irhabi 007*," *Norwegian Defence Research Establishment FFI-rapport* 02729 (2007). Available at http://rapporter.ffi.no/rapporter/2007/02729.pdf

[16] Aaron Weisburd, "Myth, Reality and Jihadist Use of the Internet," *Internet Haganah*, 1 March 1, 2007. Available at http://Internet-haganah.com/harchives/005928.html.

[17] Evan Kohlmann, "Al-Qaida's 9/11 Anniversary Video Release Delayed Due to Technical Problems, Human Errors," *Counterterrorism Blog*, 17 September 2008. Available at http://counterterrorismblog.org/2008/09/alqaidas_911_anniversary_video.php.

[18] Adam Rawnsley, "'Spyware' Incident Spooks Jihadi Forum," *Danger Room*, 1 September 2011. Available at http://www.wired.com/dangerroom/2011/09/jihadi-spyware/

[19] Aaron Weisburd, "Password-Protecting the Forums [al-Shmukh and at-Tahadi]," *Internet Haganah*, 7 January 2011. Available at http://Internet-haganah.com/harchives/007134.html.

[20] Thomas Hegghammer, "The History of the Jihadi Forums," *Jihadica Blog*, 4 March 2009. Available at http://www.jihadica.com/the-history-of-the-jihadi-forums/

[21] "Announcement on the Opening of a New Jihadi Forum," Atahadi Forum. Available at http://www.atahadi.com/vb/showthread.php?p=123672 (accessed 29 September 2010).

[22] ICT's Jihadi Websites Monitoring Group, "Periodical Review," *ICT's Jihadi Websites Monitoring Group* 1 (November 2010). Available at http://www.ict.org.il/Portals/0/Internet%20 Monitoring%20Group/JWMG_Periodical_Review_October_2010_No_1.pdf (accessed 17 May 2011).

[23] MEMRI, "Post on Al-Falluja: How to Tell if Your Jihad Recruiter is an FBI Agent,*" Jihad & Terrorism Threat Monitor* 2772 (27 January 2010) (by subscription).

[24] Combating Terrorism Center at West Point, *The Islamic Imagery Project. Visual Motifs in Jihadi Internet Propaganda* (West Point: Department of Social Sciences—United States Military Academy, 2006). Available at http://www.ctc.usma.edu/imagery/imagery_pdf.asp (accessed 17 May 2011).

[25] Nonetheless, the possibility of a link of some kind between the leaders of the Abu Hafs Brigades and the perpetrators of a number of acts of terrorism in recent years cannot be ruled out entirely. Among the most interesting cases of a connection of this type are the Madrid bombings of 11 March 2004. See Fernando Reinares, "The Madrid Bombings and Global Jihadism," *Survival* 52(2) (2010), pp. 83–104.

[26] Abu Hafs Al Masri Brigades, "Communiqué Sent to Europe on the Eve of the Imminent End to the Ceasefire Offered by Osama Bin Laden," *Asharq Al Awsat* 2 July 2004 (in Arabic).

[27] Northeast Intelligence Network, "Voice of Jihad. Issue 14 Summary and Analysis," *Northeast Intelligence Network* 7 April 2004 (by subscription).

[28] Aaron Weisburd, "It's the Thought that Counts...," *Internet Haganah*, 15 June 2011. Available at http://internet-haganah.com/harchives/007361.html (accessed 13 October 2011).

[29] Eric Schmitt and Thom Shanker, *Counterstrike: The Untold Story of America's Secret Campaign Against Al Qaeda* (New York: Times Books, 2011), p. 148.

[30] Ellen Nakashima, "Dismantling of Saudi-CIA Web Site Illustrates need for Clearer Cyberwar Policies," *The Washington Post* 19 March 2010.

[31] Although the newspaper report did not name the forum, it was probably *al-Hesbah*, which suddenly went offline in November 2008. As mentioned earlier, this forum had already been the source of controversy when its credibility was challenged by another reputed *Jihadist* forum. Furthermore, two years earlier, the Saudi authorities had arrested one of its top administrators and may have taken control of the site without users realizing. See Thomas Hegghammer, "Spy Forums," *Jihadica Blog* 19 March 2010. Available at http://www.jihadica.com/spy-forums/

[32] Bart Olmer, "AIVD lokt radicale moslims op website," *De Telegraaf* 7 August 2010.

[33] Mohammed Ali Musawi, *Cheering for Osama: How Jihadists use Internet Discussion Forums* (London: Quilliam Foundation, 2010). Available at http://www.quilliamfoundation.org/index.php/component/content/article/700 (accessed 17 May 2011).

34. Adam Rawnsley, “Taliban Webmaster: We’ve Been Hacked!,” *Danger Room*, 10 June 2010. Available at http://www.wired.com/dangerroom/2010/06/taliban-webmaster-weve-been-hacked/#more-25927#ixzz0qU3eoF5Z

35. Jarret Brachman, “High-Tech Terror”; Brian Fishman, and Joseph Felter, “The Power of Truth?: Questions for Ayman al-Zawahiri,” *Counter Terrorism Center (CTC) at West Point*, April 2008. Available at http://www.ctc.usma.edu/wp-content/uploads/2010/06/Power_of_Truth_4-21-2008.pdf (accessed 13 October 2011).

36. Institute of Counterterrorism (ICT), “The Jihadi Forums: An Open Forum with Abu Muhammad Al-Maqdisi,” *ICT’s Jihadi Websites Monitoring Group*, February 2010. Available at http://www.ict.org.il/Portals/0/Internet%20Monitoring%20Group/JWMG_Open_Forum_Abu_Muhammad_Al-Maqdisi.pdf (accessed 17 May 2011).

37. Institute of Counterterrorism (ICT), “Jihadi Websites Monitoring Group—Periodical Review,” 2 (2010). Available at http://www.ict.org.il/Portals/0/Internet%20Monitoring%20Group/JWMG_Periodical_Review_June_2010_No._2.pdf (accessed 17 May 2011).

38. Steven Stalinsky, “Deleting Online Jihad and the Case of Anwar Al-Awlaki: Nearly Three Million Viewings of Al-Awlaki’s YouTube Videos—Included Would-Be Christmas Airplane Bomber, Fort Hood Shooter, 7/7 London Bomber, and Would-Be Fort Dix Bombers,” *MEMRI, Inquiry and* Analysis Blog, 30 December 2009. Available at http://www.memri.org/report/en/print4564.htm

39. Daniel Kimmage, “Fight Terror with YouTube,” *The New York Times* 26 June 2008.

40. “The Mujahideen Don’t Target Muslims,” Consortium for Strategic Communication. Available at http://comops.org/journal/wp-content/uploads/2009/12/gadahn-mujahideen-dont-target-muslims.pdf (accessed 25 May 2011).

41. “The Mujahideen Don’t Target Muslims, Part 1,” YouTube. Available at http://www.youtube.com/watch?v=ftoSBdzcqqQ (access 12 November 2010).

42. Jarret M. Brachman and Alix N. Levine, “You Too can be Awlaki!,” *The Fletcher Forum of World Affairs* 35(1) (2011), pp. 25–46.