Routledge
Taylor & Francis Group

Studies in Conflict & Terrorism

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

Combating Terrorism in the New Media Environment

John Curtis Amble

To cite this article: John Curtis Amble (2012) Combating Terrorism in the New Media Environment, Studies in Conflict & Terrorism, 35:5, 339-353, DOI: 10.1080/1057610X.2012.666819

To link to this article: http://dx.doi.org/10.1080/1057610X.2012.666819

Studies in Conflict & Terrorism, 35:339–353, 2012

ISSN: 1057-610X print / 1521-0731 online
DOI: 10.1080/1057610X.2012.666819

Routledge
Taylor & Francis Group

Combating Terrorism in the New Media Environment

JOHN CURTIS AMBLE

Middle East & Mediterranean Studies
King's College London
London, UK

Since the 1990s, jihadist *terrorists have leveraged the power of the Internet in more imaginative ways than state security services charged with countering them. Terrorist groups are now harnessing the unique characteristics of the new media environment that has taken shape in the past decade, while security services struggle to conceptualize this rapidly evolving virtual landscape. But new media offers unique opportunities to these services, particularly intelligence agencies, to confront the terrorist threat. Identifying and exploiting these opportunities, both strategic and tactical, will lend critical advantage to governments in their worldwide confrontation with global* jihadists.

In 2003, prominent Al Qaeda strategist Abu Musab al-Suri released *The Call to Global Islamic Resistance*, a massive document outlining a series of suggestions for the future of the *jihadist* movement. In it, he stressed the need for Al Qaeda to restructure itself according to the notion of "*nizam, la tanzim*" or "system, not organization," an evolution toward the highly decentralized, multi-nodal network that defines Al Qaeda today.[1] Around the same time, Tim O'Reilly coined the term "Web 2.0" to explain the technology-enabled, peer-to-peer network shape that the Internet began to take after the bursting of the dot-com bubble in 2001.[2] Among the many manifestations of Web 2.0's characteristics was the emergence of new media, a nebulous conceptualization that encompasses a growing array of interactive communications systems facilitated by a rapidly expanding set of platforms. Blogs, Web forums, Facebook, Twitter, and Youtube, all linked together in innovative ways—these form the new media landscape, a direct result of the Web 2.0 revolution. The similarities between these two structural transformations, one of a transnational terrorist group and the other of the Internet, are striking. Indeed, Al Qaeda seems to have acknowledged these similarities by increasingly operating with considerable effectiveness in the new media environment. As such, Western intelligence agencies can ill afford to ignore this virtual domain in their efforts to combat terrorism. But can the characteristics of new media that make it such a powerful tool in the hands of terrorists also be leveraged by the institutions charged with countering them?

Examination of any question involving terrorism and the *jihadist* ideology requires a baseline understanding of the meaning of both terms. Agreement on a precise definition of

Received 24 December 2010; accepted 6 November 2011.

The views in this article are those of the author and do not necessarily represent those of the U.S. Army, the Department of Defense, or the U.S. Government.

Address correspondence to John C. Amble. E-mail: john.amble@kcl.ac.uk

terrorism is difficult to achieve among the scholars, analysts, policymakers, and security officials who all have an interest in developing one. For the sake of clarity, this article will define terrorism as "politically motivated violence that intentionally targets civilians and non-combatants," a definition that has been employed by the United Nations Security Council and endorsed by the UN Secretary General.[3] Additionally, in order to properly frame this discussion within the bounds of contemporary Western counterterrorism efforts, this article's attention is restricted to the use of terrorism by non-state actors.

While terrorism describes a particular method used to advance a set of objectives, it is employed by a wide array of entities with enormously varied goals. The analysis herein restricts its focus to *jihadist* terrorists. While *jihad* in its most fundamental form refers to an internal spiritual struggle, it has been co-opted by militants to bind together all aspects of their violent campaign against the perceived enemies of Islam. *Jihadism*, by comparison, is a neologism used to describe these militants' ideology, including its embrace of violence and total commitment to Islam's victory over apostate regimes and non-Muslim power and influence in the world.

These definitions established, it is also important to form an understanding of the term "new media." Many attempts to do so focus narrowly on only one aspect—its structure, technological characteristics, platforms, associated hardware, or its social implications. But new media's tendency to evolve with astonishing rapidity discourages such limitations. Thus, new media should be broadly defined to include the virtual networks through which so-called many-to-many communication occurs; the specific platforms that facilitate such interactions, including blogs, Web forums, social networking websites, applications that allow the sharing of user-generated content, and so on; the Web-enabled devices that allow users to tap into these networks; and new media's interactive, collaborative nature.

It is this last feature that is most relevant to this article's analysis. An investigation of new media's value in combating the terrorist threat posed by radical *jihadists* must take into account the particular social characteristics of new media. It is these transformational features that have made new media a powerful weapon in the hands of terrorists but also hold immense potential for government agencies charged with meeting and defeating the terrorist threat. Chief among new media's revolutionary impacts on the information environment is the advent of many-to-many systems of communications. Traditional media is characterized as "one-to-many" communication, where the audience might be virtually limitless, but a small cohort of established institutions selectively disseminate information. New media, by contrast, substitutes these institutions with the same unlimited universe from which audiences were previously drawn. In essence, new media allows information consumers to also act as communicators, yielding a vast expansion in the number of information transmitters present in the media landscape.

This expansion has also led to the creation of virtual networks of likeminded individuals who choose to receive information from the same sources, and allows particular communicators to reach members of these networks. In economic terms, the transformation of the Internet has made a new generation of businesses profitable by allowing access to small, diffused sets of customers in the market for very specific items (demographic groups that writer Chris Anderson has coined the "Long Tail").[4] This logic also explains how barriers to entry into ideological markets are equally reduced.[5] As a result, a strong element of social cohesion can be formed among geographically dispersed adherents to even the most extreme worldviews.

As devotees of particular ideologies selectively consume information, this virtual cohesion gains further traction and an additional phenomenon of the new media environment emerges: crowd-sourcing. The sense of group membership that builds as individuals identify

more and more strongly with a particular ideology encourages greater active participation on behalf of that ideology. Terrorist groups have been adept at exploiting this phenomenon, particularly with respect to training and propaganda. No longer are such groups limited to in-house expertise on topics from explosives to media production. They can now avail themselves of critical, and in some cases highly refined, skill sets of supporters around the world. This, as will be shown, is just one of many ways in which terrorists have skillfully taken advantage of the emergence of new media.

Terrorist Use of New Media

As the weaker contestant in an increasingly global struggle, *jihadist* terrorists were quick to note the Internet's equalizing function as early as the 1990s. Their ability to leverage the Internet, paired with the degradation of the state's previous near-monopoly of information flow, was predicated on the coincidence of four factors, according to Thomas Rid and Marc Hecker: reduced computing prices; improved digital technology; increased bandwidth capacity; and expansion of Internet penetration worldwide.[6] This last factor is particularly important, as penetration is growing at tremendously rapid rates in those parts of the world where the resonance of the *jihadist* narrative of Western subjugation of Muslims is greatest. Between 2000 and 2011, Internet connectivity grew by 480 percent worldwide.[7] Figures for the Middle East show a growth of nearly 2,000 percent, while Internet penetration expanded in Pakistan by a staggering 15,000 percent. Among the earliest attempts by *jihadists* to explore the Internet's power was the establishment of Azzam.com in 1997 by a student at Imperial College in London.[8] Developed to publicize *jihadist* fighters around the world, it would be described by terrorism expert Evan Kohlmann as "the very first real al Qaida Web site."[9] Other groups would soon mimic this template. In 1998, fewer than fifteen terrorist organizations had an online presence; between 2003 and 2005, a study found that the online terrorist landscape had exploded to more than 4,300 terrorist sites.[10] The reason for this vast expansion in online terrorist activity can be explained largely by the unprecedented control of message content and communications made possible in the lawless, diffused online world.[11]

Terrorists' use of the Internet has grown further in the wake of the Web 2.0 revolution as they have adopted new ways of leveraging the unique features of new media. In *The Call to Global Islamic Resistance*, al-Suri "frequently discusses the Internet and new media technologies, recognizing them as critical vehicles for inciting global resistance," notes terrorism analyst Jarret Brachman.[12] This raises the important question of *why* new media technologies are critical to Al Qaeda's strategic communications efforts. The answer lies in the characteristics of the Internet's transformation over the past decade. Just as this transformation has given commercial enterprises access to Anderson's "Long Tail" of consumer markets, new media technologies provide an avenue through which to communicate with a small, diffused market of potential *jihadist* operatives and supporters. Savvy *jihadist* strategists have been quick to exploit new media to this end. In the 1990s, Europe-based supporters of the Algerian *Groupe Islamique Armé* required considerable financial and labor investments to produce their *al-Ansar* newsletter in hardcopy form and disseminate it around the world.[13] Today, increasing Internet penetration and the crowd-sourcing function of new media guarantee that *jihadist* messages reach geographically dispersed audiences more quickly and with fewer dedicated resources than ever before.

Indeed, some terrorist groups and active supporters have become so comfortable operating in the new media environment that they have established a presence on popular social networking sites. A 2009 report compiled by the Simon Wiesenthal Center found a number

of terrorist-related Facebook groups, including one called "HAMAS Fans" and another titled "Support Bin-Laden(Al-Qaeda)—Eradicate the West!!!!"[14] Perhaps the most telling illustration of the convergence of technology, new media, and *jihadism* was uncovered in the wake of the December 2010 suicide bombing in Stockholm. After blowing himself up, Taimour Abdulwahab al-Abdaly's Facebook profile showed that his "likes" included "the Islamic Caliphate state," "Yawm al-Qiyamaah (the Islamic day of judgment)," and "I love my Apple iPad."[15]

An analysis of terrorist use of new media reveals four principal areas in which the new technologies have most greatly enhanced their capabilities: propaganda, recruitment, training, and operational command and control. While combatant groups employ propaganda for varying purposes, its value for terrorists specifically lies in the magnification of public attention to their cause and their activities. Militarily weak organizations cannot hope to achieve strategic objectives by force alone. Their chances for success, and indeed their very relevance, hinge enormously on earning and maintaining popular support, making the psychological battle supremely important for *jihadists*. For them, a failure to adopt powerful new weapons can have catastrophic impacts. As such, terrorists have embraced new media technologies to spread their messages.

Key to Al Qaeda's chosen strategy to win the broader conflict with the West is the development of a shared sense of identity among the *ummah*, the global Muslim community, encouraging the internalizing of suffering endured by Muslims anywhere in the world. Video has become a critical tool for terrorists to psychologically bind large segments of the world's Muslim population together by this method. An example can be seen in the video of 7/7 bomber Mohammed Siddique Khan released by Al Qaeda after the attacks. In it, the Leeds-born British citizen claims that his pending attack in London is a necessary act, because "democratically elected governments continuously perpetuate atrocities against *my people* all over the world."[16] Videos of attacks on Western military forces in Iraq and Afghanistan have furthered this argument, depicting the actions of dutiful Muslims defending local communities from conquest by armies of non-Muslim invaders.

The method by which these videos are produced, edited, and distributed is particularly relevant to this article's analysis. Because there is no evidence that financial incentives play a role in this process, the creation and viral dissemination of *jihadist* propaganda cannot be explained by market-based or firm-based production models. Instead, propaganda video production takes form through a type of non-proprietary collaborative system.[17] While traditional production models struggle to grasp the nature of such a system, it is predicated on the same logic that explains the success of Wikipedia and other major landmarks in the new media environment. Essentially, nontraditional motives encourage participation in producing and improving content. By tapping into these individual motives—be they antigovernment grievances, relatively normal youthful discontent, or any other—*jihadist* propagandists have been able to create decentralized networks of users who can incrementally improve a video production by applying personalized skill sets. These media networks can then be merged with operational networks of terrorist groups around the world. As Daniel Kimmage writes in *The Al-Qaeda Media Nexus*, "Virtual media production and distribution entities (MPDEs) link varied groups under the general ideological rubric of the global jihadist movement."[18] Among the most prominent of these virtual entities is the Global Islamic Media Front (GIMF). In a 2004 article in the London-based magazine *al-Sharq al-Awsat*, Dr. Hani al-Siba'i predicted that the newly formed GIMF ". . . . will attract small groups from all over the world and this will strengthen it so that if the media section of any group is hit, this will not impede the overall media process. . . ."[19]

Propaganda helps terrorist groups to both radicalize potential supporters and recruit individuals to their cause, the second area in which new media's value to terrorists is apparent. Potential recruits can meet likeminded individuals on social networking sites, communicate with recruiters via interactive forums, and access propaganda materials from file-sharing websites. Most participants in *jihadist* online activity are unlikely to ever conduct a violent attack. Many play other roles, such as editing and disseminating terrorist media. But even among this group there are supporters who exhibit an enormous commitment to the *jihadist* cause. In 2004 and 2005, an online media operative with the screen name Irhabi007 earned virtual celebrity status on extremist Web forums by his adroit use of new media platforms to distribute *jihadist* propaganda.[20] Irhabi007, later identified as Younis Tsouli, was arrested in late 2005 and charges were filed based on his extensive online activities in support of Al Qaeda. Investigation into Tsouli's activities revealed that although he contributed greatly to terrorist efforts through his online work, he also lamented these auxiliary responsibilities and yearned for the opportunity to join Al Qaeda fighters in Iraq.[21] Tsouli's use of new media to broadcast Al Qaeda propaganda to vast audiences demonstrates its capacity to facilitate radicalization. His own desire to play a more active real-world role shows how immersion into a fanatical virtual environment encourages total commitment and aids in recruitment of individuals prepared to engage in terrorist violence.

The third major way in which terrorists use new media is for training purposes. The sheer quantity of instructional materials distributed via interactive Web forums attests to such platforms' usefulness for terrorist training. Hsinchun Chen leads the Dark Web Terrorism Research project at the University of Arizona, which collects and analyzes information related to terrorists' use of the Internet. The project has identified tens of thousands of Improvised Explosive Device (IED)–related postings alone. According to Chen, "there is a lot of IED information generated by terrorists everywhere—websites, forums, people telling you where to buy fertilizer and how to plant IEDs."[22] Al-Ekhlaas, a forum that served as one of the primary nodes in global *jihadists*' propaganda distribution network, has hosted instructional information on the construction of cell-phone detonators.[23] And *Inspire* magazine, an English language electronic publication produced by Al Qaeda's affiliate in the Arabian Peninsula and disseminated via hyperlinks spread across the virtual *jihadist* landscape, has included instructional articles such as "Make a Bomb in the Kitchen of your Mom."[24]

The emergence of new media platforms that facilitate the publication and transfer of such training materials came at a critical juncture for terrorist groups. The 2001 invasion of Afghanistan stripped Al Qaeda and a number of associated groups of the main territory where training camps were located. Although some camps continue to operate across the border in Pakistan, a surge in drone strikes has made ongoing training operations increasingly difficult there, too. Terrorist groups have made up for this loss of physical territory by transplanting training activities into the online world. *Inspire* magazine's second edition directly discourages supporters from traveling overseas to join the *mujahideen*. The magazine instead suggests a number of attacks that can be executed in the readers' home countries and offers an array of both rudimentary and complex instructional materials to avoid the need for real-world practical training.[25]

The fourth way new media bolsters terrorist efforts is by enhancing their ability to exercise command and control of specific operations. While there are fewer examples of terrorists' use of new media tools for this purpose compared to propaganda, recruitment, and training, it represents the most direct application of the innovative platforms to terrorists' violent activities. Specifically, new technologies facilitate immediate communication between a range of Web-enabled devices. The invention of the telegraph in the early

nineteenth century heralded the era of centralized command and control for state-based armies.[26] The expansion of interactive, Web-based technologies has had a similar effect for terrorist organizations. Equipped with handheld devices and using Voice Over Internet Protocol applications to communicate, the perpetrators of the 2008 attacks in Mumbai, for instance, were able to systematically coordinate their movements to maximize the bloody effects of their violent rampage.[27]

These four areas—propaganda, recruitment, training, and command and control—provide the clearest examples of how terrorists have ably exploited new media technologies. However, the full extent of their use of new media can best be appreciated only when governments' comparative failure to employ these tools to combat terrorism is understood.

Governments' Failure to Adopt New Media Tools

The past decade and a half has seen the Internet pervade virtually all aspects of society. During this same period, terrorism has developed into arguably the most visible security priority for governments. As such, security agencies were eager to harness emerging Internet technology to combat the threat of terrorism. But while terrorist groups would undertake a wide range of activities online, Western militaries and intelligence organizations would apply new technologies much more narrowly. Two important assessments can be made regarding governments' narrow view of the Internet's counterterrorism utility. First, states have employed connectivity-related technology primarily to enhance internal communication. Any function of external communication or monitoring of terrorist groups and their supporters was considered secondary and largely ignored. Secondly, while security officials acknowledged the Internet's potential as a force multiplier, little emphasis was placed on stopping terrorists from using it to bolster their own capabilities. John Arquilla argued as recently as 2009 that this remains a problem: "... none of the key military, intelligence, and law-enforcement arms of the US government have done much to curtail terrorist use of the Net."[28]

As with this relatively narrower view of the utility of the Internet compared to that of terrorist organizations, state security agencies' collective approach to new media is also worryingly limited. The institutional and bureaucratic challenges governments face in adapting quickly and efficiently to rapid changes in threats, operational environments, and collection priorities also limit their ability to react to technological evolutions in the information domain. Donald Rumsfeld wrote in 2006 that "our enemies have skillfully adapted to fighting wars in today's media age, but for the most part we ... have not."[29] The U.S. Intelligence Community (IC) has clearly recognized the value of new media technologies, albeit only in limited circumstances. Intellipedia serves as a collaborative repository of classified intelligence from which professionals throughout the community can draw.[30] IC analysts can also share information on A-Space, another creation developed to harness the networking power of new media by mirroring processes and platforms used widely on popular social networking sites.[31] Yet when it comes to employing new media technology for purposes other than internal communications, intelligence and defense officials appear primarily concerned with the potential for operational security lapses caused by soldiers and IC employees with blogs or Facebook profiles.[32] In sum, those bodies charged with countering terrorism have inadequately leveraged new media in support of this mission.

A full appreciation of the opportunities lost by this limited approach requires an understanding of the nature of the conflict between governments and their terrorist adversaries itself. The early years of the U.S.-led response to the 9/11 attacks, which formally propelled

counterterrorism to the top of Western governments' list of security priorities, were characterized by strictly kinetic operations reliant on overwhelming technological superiority. These "capture/kill" operations sought to target individual members and leaders of the Al Qaeda movement, mostly those based in the mountainous, ungoverned spaces along the border between Afghanistan and Pakistan. This approach would dominate Western counterterrorism thinking in the early years of the war in Afghanistan, according to observers such as journalist Ahmed Rashid.[33] But in 2003, James Carafano coined the phrase "the long war," arguing that this strictly military response would be just one small piece of a much longer battle against the *jihadist* ideology that spawns terrorism.[34] Recent years have seen Western governments pursue a two-pronged approach, attempting to pair tactical battlefield successes with a concerted "hearts and minds" campaign aimed at vulnerable populations. The U.S. government, for example, promotes education, healthcare, and other aid programs in *jihadist* recruiting grounds of Muslim countries. At the same time, it has stepped up drone strikes against top militants in Pakistan, Yemen, and Somalia. Defeating the terrorist threat will require this careful combination of kinetic operations and a long-term strategic commitment to confronting the violent ideology.

While governments clearly appreciate the need to pursue objectives on both tactical and strategic levels in order to combat the threat of terrorism, they have not yet incorporated new media's unique features into a comprehensive counterterrorism plan. At a tactical level, new media has not yet gained traction as a legitimate source of intelligence. Speaking of the 2006 war between Israel and Hezbollah, an Israeli Defense Forces spokesperson dismissed Web-only intelligence sources, arguing that they cannot be trusted.[35] But uncertainties regarding the credibility of sources plague all intelligence collection disciplines to varying degrees, particularly human intelligence (HUMINT). Evaluating source credibility is a key component of the intelligence analytical process. As with HUMINT sources, the credibility of each Internet-based source can be gauged based on past reporting accuracy, an assessment of the source's placement vis-à-vis key targets, and an array of other factors. Based on the earlier examples of terrorists' use of Web forums, social media tools, and other technologically innovative communication platforms, failure to treat these as legitimate intelligence sources leaves governments at a distinct tactical disadvantage.

On a strategic level, despite governments' growing emphasis on the long-term ideological component of their fight to combat terrorism, they too often approach it without leveraging the valuable features of new media tools. For example, in early 2011, the U.S. military acknowledged its development of software applications to create credible virtual identities to shape online conversations.[36] The tool was intended to provide an ideological counter to *jihadist* propaganda and plans called for the personas to use Arabic, Farsi, Urdu, and Pashto languages. The military, however, has specifically stated that it was not targeting either Facebook or Twitter. While the program itself was criticized among some segments of the media, implementing it with such limitations seriously diminishes its capacity to achieve its stated objectives. U.S. psychological operations (PSYOP) regulations also suggest a failure to recognize how new media has changed the landscape on which ideas compete with each other. PSYOP product approval responsibility is retained by the Under Secretary of Defense for Policy and delegation below any of the military's ten combatant commanders requires explicit approval by the Secretary of Defense.[37] This centralization of information control is an institutional hallmark of militaries and other large government agencies, but it is antithetical to the cultural shifts in communication associated with the Web 2.0 revolution.

Because of governments' limited use of new media to enhance their efforts to combat the threat of terrorism, it is clear that they forfeit a variety of benefits. But what are the

specific strategic and tactical advantages new media holds for those agencies charged with a counterterrorism mandate, and how can governments best exploit them?

New Media's Strategic and Tactical Advantages

At a strategic level, the struggle between terrorists and governments is best understood as an ideological confrontation. As such, parallels between today's security challenges and the Cold War are often drawn. But whereas the Cold War evolved into a conflict for influence among governments throughout the world, today's battle against the *jihadist* ideology is best understood as a fight for influence in the minds of individuals. Much of this fight will take place in the virtual realm. According to Al Qaeda's strategist al-Suri, because of America's "stunning technological superiority," the "'Tora-Bora mentality' has to end."[38] For Al Qaeda, the fight could not be won if it were for geographic territory alone, and must move into the domain of human influence. As discussed earlier, new media would play a prominent role in the group's new strategy. Counterterrorism efforts cannot afford to ignore this new virtual battlefield. As former homeland security advisor to the U.S. government, Chris Battle, has written:

> . . . those who continue to dismiss the power of New Media sources to enhance planning and coordination—not to mention its most powerful capability, which is to magnify public attention to [terrorists'] cause—are either delusional or compensating for their own failure to stay ahead of the curve.[39]

Just as new media lends terrorists the ability to magnify public attention to their cause, it can serve the same purpose for governments seeking to highlight activities that might generate goodwill among populations vulnerable to radicalization. To suggest that the ideological battle with *jihadism* is entirely binary is overly simplistic. Merely winning over members of particular communities is not sufficient to keep the *jihadist* threat at bay. But such an effect would make it exceedingly difficult for Al Qaeda's narrative that the West is at war with Islam to take root in what might otherwise be fertile ground. In Pakistan, the percentage of the population holding favorable views of the United States dropped from 17 percent in July 2010 to 12 percent in June 2011, according to reports by the Pew Research Center.[40] Yet this drop in pro-U.S. sentiment coincided with a period in which the U.S. government contributed nearly 700 million dollars in relief aid in response to the July 2010 floods that ravaged much of Pakistan, more than a quarter of total international assistance.[41] A systematic effort to utilize new media platforms to publicize this fact could have played a major role in fostering positive feelings of the United States and other donor nations within a population susceptible to radicalization.

Those who would argue that limited technological infrastructure would inhibit the usefulness of such a strategy do so from a weak position. Internet penetration, as shown, is growing most rapidly in these areas, bringing access to new media tools to ever expanding territories. Indeed, the May 2011 raid that killed Osama bin Laden was shrouded in every bit of secrecy the U.S. government could muster. Yet the first public reflections of the raid came in a Twitter post from an Abbottabad resident, who noted the rarity of a helicopter hovering in the area in the middle of the night and followed this initial message with several more updates in real time.[42] It is clear, then, that using new media to communicate with critical target audiences is feasible. Doing so holds great potential to help enhance the reputation of Western democracies and offer alternatives to *jihadist* narratives in the strategic confrontation with terrorism.

Offering these alternatives and promoting countermessages is an important step in degrading the influence of the *jihadist* ideology. Historically, this has been an important role of intelligence agencies. During the Cold War, the CIA covertly funded the Congress for Cultural Freedom, an organization through which leading leftist intellectuals could voice anti-Soviet opinions.[43] The agency also arranged for a secret 1956 speech in which Nikita Khrushchev attacked the cult of personality that had arisen around the memory of Stalin to be published in newspapers around the world, exposing cracks in the façade of Soviet ideological unity.[44] Today's intelligence agencies can leverage new media technologies to exploit similar divisions among their terrorist adversaries. Analysts define a number of sub-schools of Salafist ideology, for instance, of which violent *jihadism* is only one. Highlighting this diversity and promoting alternatives to *jihadism* will be a critical element in the strategic confrontation with terrorism. Senior Al Qaeda figure Abu Yahya al-Libi alluded to this vulnerability in a 2007 video. He acknowledged that amplifying the voices of former *jihadists* who have renounced violence would be a particularly effective strategy to counter his organization.[45] But in order to be effective, these messages need to be placed in direct competition with *jihadist* propaganda across the new media environment.

The propaganda that governments must seek to counter targets a wide variety of audiences. Among the most important, from the perspective of intelligence agencies, are disaffected Muslims living in the West. Terrorist targeting of this group with media is similar to Soviet subversion activities during the Cold War, at least insofar as both were oriented toward destabilizing objectives. Countering subversion is even more critical in today's ideological battle against violent *jihadism* than it was in the decades-long fight against communism. In order for Soviet subversive tactics to yield success, a critical mass of support needed to be discretely generated within Western societies. *Jihadist* subversion is successful if its propaganda motivates a single individual to conduct a terrorist attack. Terrorism expert Bruce Hoffman wrote in 2010 that ". . . seeking recruits from non-Muslim countries who can be easily deployed for attacks in the West" represents one of five key elements of Al Qaeda's newest strategy.[46] But a program that focuses exclusively on identifying those already radicalized and planning attacks is problematic, comparable to a Cold War–era emphasis on only those Westerners who have been successfully targeted by Soviet subversion, rather than striving to defeat the networks behind the subversive activity itself. Thus, intelligence agencies must aim to fully grasp the nature of terrorist subversion in the West so that it can be effectively contained and ultimately defeated. Ongoing efforts to identify the particular Web forums and other new media platforms that are instrumental components of terrorist propaganda networks represent an important step toward defeating the subversive threat. But it is critical that these efforts form part of a broader strategy specifically designed to undermine radicalization processes and combat the *jihadist* ideology.

In addition to its strategic value in the confrontation with the *jihadist* ideology—Carafano's "long war" mentioned earlier—new media also holds considerable potential to aid Western intelligence agencies in the day-to-day battles against terrorist operatives. As terrorists increasingly rely on new media for training and operational support, the monitoring of critical communications platforms is growing in importance. Governments are increasingly aware of this tactical value, but they must often overcome an innate institutional conservatism in order to take full advantage. As highlighted earlier in this article, information gleaned from Web-based resources is often not trusted and there is a troubling resistance to treating new media as a fully legitimate source of intelligence.

Overcoming this resistance and developing a virtual presence that spans the new media landscape will allow governments to glean important pieces of information during

crises. As the use of popular communications and information-sharing platforms continues to grow throughout the world, the experiences and unique perspectives of individuals are increasingly broadcast in real time. As was shown earlier in this article, attackers in Mumbai used new media tools to maximize the effects of their violent rampage. But new media also offered some of the earliest pieces of critical information necessary for security agencies to develop a picture of events as they unfolded. Posts to the widely popular mini-blogging platform Twitter provided the first indication that Americans and Britons were being specifically targeted, and photo-sharing site Flickr hosted images of the attackers taken in the early moments of the attack.[47] Such applications thus have the potential to serve as powerful tools for counterterrorism agencies. Sifting through the massive amount of information will pose an immense challenge. Twitter users post "tweets" at a rate of 250 million per day, and this number is growing rapidly.[48] But while this massive figure poses serious difficulties from an information management perspective, it also represents an enormous expansion in the number of information sources from which security agencies can draw critical updates during a time of crisis. Development of effective mechanisms to collect and analyze such information will offer governments an important advantage when facing immediate threats.

Jihadist propaganda videos, produced collaboratively and disseminated virally with the help of new media platforms, also provide a window through which governments can observe terrorist tactics, techniques, and procedures. A common video format used to recruit (and perhaps desensitize) potential operatives and supporters includes video footage of *jihadist* attacks, often conducted in Afghanistan. Such videos reveal key terrorist methods and should be scrutinized to facilitate the development of countermeasures. In the United States, monitoring the outlets that host these videos has become the responsibility of the CIA's Open Source Center (OSC). In a 2007 speech, OSC director Doug Naquin said, "We're looking now at YouTube, which carries some unique and honest-to-goodness intelligence."[49] The raw information that can be gleaned by monitoring terrorist media releases is demonstrated by a video disseminated after a 2004 attack in Riyadh, Saudi Arabia. In addition to pre-filmed statements by the suicide operatives, the video contained revealing footage of important preparations, including the loading of explosives into the vehicle used in the attack.[50] This imagery is immensely useful to intelligence agencies' experts tasked with developing an understanding of technical procedures employed by terrorist groups.

Incorporating new media platforms into existing practices can also enhance HUMINT collection. The case of Younis Tsouli, the man behind the online pseudonym Irhabi007, offers an instructive example. What if, instead of being arrested and charged, Tsouli had been somehow made to serve as a conduit through which British security agencies could extract valuable intelligence from the terrorist forums that he accessed frequently and, in some cases, administered? The particular method most likely to have secured Tsouli's cooperation, whether persuasive or coercive, is beyond the scope of this article. Western intelligence officers successfully employed both approaches during the Cold War, which leads to an important question: can traditional HUMINT tactics be adapted to fit the new media environment? In his 2008 book, *Why Spy? Espionage in an Age of Uncertainty*, former CIA inspector general Frederick Hitz argued that the capacity of HUMINT to offer concrete value to intelligence agencies has not diminished. But its effectiveness depends on an acknowledgement that "... the spy universe is no longer adequately defined by 'foreign countries.' It includes Al Qaeda or the Taliban or the Iraqi insurgents ... whatever transnational group is engaged in hostile action against Western interests."[51]

As the potential targets of HUMINT collection have changed, so too has the operational environment become increasingly virtual. But even in this virtual environment, Rid and Hecker argue, the true nature of the transformation associated with emerging Web 2.0 technologies is more cultural than technological.[52] This suggests that perhaps HUMINT collection is better suited to the new media environment than intelligence agencies seem to recognize.

In *The Craft of Intelligence*, former CIA Director Allen Dulles describes the two primary methods of covert HUMINT collection as penetration and recruitment of "agents in place."[53] Each method is marked by particular characteristics that make it potentially useful in collecting against online targets in a virtual space. Internet-based communication platforms, including Web forums in which participants' real identities are obscured by screen names, have evolved within a culture of pseudonymity.[54] This often overlooked fact makes terrorist targets in the virtual world vulnerable to covert penetration. In traditional HUMINT operations, a penetrating agent must be provided with a detailed profile that can withstand considerable scrutiny. In the pseudonymous virtual world, however, this profile can quite literally be built simply by creating a screen name and adopting suitably extreme rhetoric.

During the Cold War, inability to penetrate a target left intelligence officers with the alternative of recruiting an asset with preexisting access.[55] This is the means of collection that would have been employed had Younis Tsouli been either coerced or persuaded to relay information to British security services. Securing the cooperation of an individual with established credibility among the online *jihadist* community would provide intelligence agencies with a source of greater immediate value than would be available through direct insertion of an outside agent. Intelligence scholar Michael Herman goes so far as to argue that ". . . informers provide almost the only means of penetrating non-state terrorism."[56]

Besides providing intelligence agencies with valuable information, HUMINT collection—whether undertaken by means of penetration or recruitment—can have other positive implications from the perspective of counterterrorism officials. While collection is designed to be highly secretive, any suspicion of its existence can create a strong sense of mistrust among online *jihadists*. History is replete with examples of movements whose end was brought nearer by a paranoid obsession with subversive elements and informers, particularly within ideologically rigid organizations. In 1938, Stalin demanded an operation to purge anti-Soviet elements from Soviet society, one of many such actions, ordering the arrest of 57,200 people across the country.[57] These purges often targeted members of his inner circle who had not displayed any sign of working to undermine the Soviet regime, a destructive impulse that would severely hamstring the Soviet government. A similar effect among *jihadists* would seriously degrade the operational abilities of groups like Al Qaeda, which should form a primary objective of Western intelligence agencies.

Recommendations

Having examined the past approaches to the Internet and new media by both state security services and their terrorist adversaries, identifying opportunities for intelligence agencies to harness the power of new media technologies to combat terrorism on both strategic and tactical levels, a few key policy prescriptions can be made:

1. *Pursue structural decentralization to leverage junior IC members' inherent new media literacy.* Young intelligence officers and analysts are "digital natives," having

come of age in the era of computerized interconnectivity. As such, they possess a more nuanced and intuitive sense of the powers of new media than the "digital immigrants" who fill upper echelon positions. Specific measures should be taken to guarantee their role in conceptualizing novel approaches to the use of constantly evolving technologies.

2. *Develop a target-centric approach to monitoring* jihadist *media output.* Intelligence agencies have developed refined targeting methodologies that support a wide range of operations, from kinetic strikes to infrastructure destruction to target surveillance. These targeting techniques can greatly increase the effectiveness of monitoring of the rapidly expanding and increasingly complex online multimedia environment, and should be fully and formally applied to that end.
3. *Transform HUMINT capabilities to fit the new media environment.* HUMINT can and should play a major role in combating terrorism. Although online *jihadist* activity takes place in a virtual domain, the temptation to place collection functions exclusively within the province of cyber-focused intelligence branches should be resisted. The social characteristics of new media must be understood, covert collection efforts should be modified from existing doctrine, and adequate resources should be directed toward clandestine service branches to exploit the major vulnerabilities of online *jihadist* activity to HUMINT collection.

This list is certainly not exhaustive, and new methods will emerge for counterterrorism security services to combat extremism in the new media environment. But these recommendations provide a promising starting point from which Western governments can gain an advantage in the long-term fight against terrorism. Additionally, while it has not been addressed in this article and has been the topic of considerable analysis, information flow between various agencies must be fostered. In most Western societies, protection of civil liberties has led to clear lines of division between the foreign intelligence mandates of certain agencies and the internal security and law enforcement functions of others. While these important distinctions must remain, cooperative information sharing is necessary for security services to exploit new media in their efforts to combat an adversary that does not limit its operations based on international borders. As Hitz writes, we should see "... an increasing interdependence between foreign intelligence services like the CIA and Britain's MI-6, with their domestic security partners, the FBI, MI-5, and local police forces."[58] The 9/11 Commission identified such interagency cooperation as a principal requirement to detect and defend against future terrorist attacks.[59] The creation of the National Counterterrorism Center in response to the commission's recommendations was an important step in addressing what had become a critical deficiency in the U.S. intelligence community's structure. But such openness is threatened by misguided responses to episodes such as Wikileaks's publication of classified documents. This pendulum should not be allowed to swing broadly between the two ideals of intelligence sharing and secrecy. Interagency communication must remain the overarching objective, with adequate controls built in to manage individual threats to information security.

Making sense of the numerous threats that governments and societies face by collecting and analyzing intelligence has always been a messy task. It has become more so as new technologies have reshaped the world, adding heretofore-unfathomable layers of complexity. But by embracing these changes and fully exploiting the growing sources of information available in the new media environment, Western intelligence agencies can ensure that they face their terrorist adversaries from the strongest possible position.

Notes

1. Raffaello Pantucci, "Review Essay: Al-Qaeda 2.0," *Survival* 50(6) (2008), p. 183.
2. Tim O'Reilly, "What is Web 2.0," 30 September 2005. Available at http://oreilly.com/web2/archive/what-is-web-20.html (accessed 24 October 2011).
3. Peter R. Neumann, *Old & New Terrorism: Late Modernity, Globalization and the Transformation of Political Violence* (Cambridge and Malden, MA: Polity Press, 2009), p. 7.
4. Chris Anderson, *The Long Tail: Why the Future of Business is Selling Less of More* (New York: Hyperion, 2006).
5. Thomas Rid and Marc Hecker, *War 2.0: Irregular Warfare in the Information Age* (Westport, CT and London: Praeger Security International, 2009), p. 31.
6. Ibid., p. 29.
7. Data from "Internet World Stats: Usage and Population Statistics." Available at http://www.internetworldstats.com/ (accessed 6 October 2011).
8. David Rennie and David Millward, "The Imperial College Student Accused of Waging Jihad in South Kensington," *The Telegraph*, 7 August 2004. Available at http://www.telegraph.co.uk/news/uknews/1468854/The-Imperial-College-student-accused-of-waging-jihad-in-South-Kensington.html (accessed 7 October 2011).
9. Craig Whitlock, "Briton Used Internet as His Bully Pulpit," *The Washington Post*, 8 August 2005. Available at http://www.cs.washington.edu/education/courses/csep590/05au/readings/WA.Post.terrorism/Post2.htm (accessed 7 October 2011).
10. Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace, 2006), p. 15.
11. Maura Conway, "Terrorism and the Internet: New Media—New Threat?" *Parliamentary Affairs* 59(2) (2006), p. 284.
12. Jarret M. Brachman, *Global Jihadism: Theory and Practice* (London and New York: Routledge, 2009), p. 116.
13. Omar Nasiri, *Inside the Jihad: My Life with Al Qaeda* (New York: Basic Books, 2006), pp. 26, 40.
14. Abraham Cooper, "Facebook, YouTube +: How Social media Outlets Impact Digital Terrorism and Hate," *Simon Wiesenthal Center* (2009), pp. 9, 49. Available at http://www.wiesenthal.com/site/apps/s/content.asp?c=lsKWLbPJLnF&b=4442915&ct=6994349 (accessed 24 October 2011).
15. Jonathan Paige, "Stockholm Suicide Bomber: Taimour Abdulwahab al-Abdaly Profile," *The Guardian*, 12 December 2010. Available at http://www.guardian.co.uk/world/2010/dec/12/stockholm-suicide-bomber-profile (accessed 7 October 2011).
16. "London Bomber Video Aired on TV," *BBC*, 2 September 2005. Available at http://news.bbc.co.uk/1/hi/uk/4206708.stm (accessed 24 October 2011).
17. Rid and Hecker, *War 2.0*, p. 30.
18. Daniel Kimmage, *The Al-Qaeda Media Nexus: The Virtual Network Behind the Global Message* (Washington, DC: Radio Free Europe/Radio Liberty, 2008), p. 1.
19. Muhammad al-Shafi'i, "Fundamentalist Move toward Uniting Their Mouthpieces on the Internet under Cover of What They Call 'Islamic Media Front,'" *al-Sharq al-Awsat*, 6 October 2004, p. 5.
20. Rita Katz and Michael Kern, "Terrorist 007, Exposed," *The Washington Post*, 26 March 2006. Available at http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html (accessed 7 October 2011).
21. "A World Wide Web of Terror," *The Economist*, 14 July 2007, p. 28.
22. Thomas Frank, "Feds may Mine Blogs for Terrorism Clues," *USA Today*, 24 December 2008. Available at http://www.usatoday.com/printedition/news/20081224/terrorblogs24_st.art.htm (accessed 24 October 2011).
23. Abraham Cooper, "Facebook, YouTube +: How Social media Outlets Impact Digital Terrorism and Hate," *Simon Wiesenthal Center* (2009), p. 55. Available at http://www.wiesenthal.com/site/apps/s/content.asp?c=lsKWLbPJLnF&b=4442915&ct=6994349 (accessed 24 October 2011).

24. Richard Spencer, "Al-Qaeda newspaper: Make a bomb in the kitchen of your mom," *The Telegraph*, 1 July 2010. Available at http://www.telegraph.co.uk/news/worldnews/7865978/Al-Qaeda-newspaper-Make-a-bomb-in-the-kitchen-of-your-mom.html (accessed 17 October 2011).

25. The most direct discouragement from overseas travel appeared in the "Open Source Jihad" section of *Inspire's* second issue, pp. 51–57.

26. Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (Harlow, Essex, UK: Allen Lane, 2005), p. 70.

27. Chris Battle, "New Media's Moment in Mumbai," *Foreign Policy Journal*, 15 January 2009. Available at http://www.foreignpolicyjournal.com/2009/01/15/new-media's-moment-in-mumbai/ (accessed 17 October 2011).

28. John Arquilla, "How to Lose a Cyberwar," *Foreign Policy*, 11 December 2009. Available at http://www.foreignpolicy.com/articles/2009/12/11/how_to_lose_a_cyberwar (accessed 24 October 2011).

29. Donald Rumsfeld, "War in the Information Age," *The Los Angeles Times*, 23 February 2006. Available at http://articles.latimes.com/2006/feb/23/opinion/oe-rumsfeld23 (accessed 24 October 2011).

30. Steve Vogel, "For Intelligence Officers, A Wiki Way to Connect Dots," *The Washington Post*, 27 August 2009. Available at http://www.washingtonpost.com/wp-dyn/content/article/2009/08/26/AR2009082603606.html (accessed 24 October 2011).

31. "CIA, FBI Push 'Facebook for Spies,'" *CNN*, 5 September 2008. Available at http://edition.cnn.com/2008/TECH/ptech/09/05/facebook.spies/index.html?eref=edition (accessed 24 October 2011).

32. "Directive-Type Memorandum (DTM) 09-026—Responsible and Effective Use of Internet-Based Capabilities," Memorandum from the Deputy Secretary of Defense, 25 February 2010. Available at http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026.pdf (accessed 24 October 2011).

33. Ahmed Rashid, *Descent into Chaos: Pakistan, Afghanistan and the Threat to Global Security* (London: Penguin Books, 2009), p. 62.

34. James Carafano, "The Long War Against Terrorism," *The Heritage Foundation*, 8 September 2003. Available at http://www.heritage.org/Research/Commentary/2003/09/The-Long-War-Against-Terrorism (accessed 24 October 2011).

35. Rid and Hecker, *War 2.0*, p. 121.

36. Nick Fielding and Ian Cobain, "Revealed: US Spy Operation that Manipulates Social Media," *The Guardian*, 17 March 2011. Available at http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks (accessed 19 October 2011).

37. "Joint Publication 3-53: Doctrine for Joint Psychological Operations," 5 September 2003. Available at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/02_psyop-jp-3-53.pdf (accessed 19 October 2011).

38. Rid and Hecker, *War 2.0*, p. 190.

39. Chris Battle, "New Media's Moment in Mumbai," *Foreign Policy Journal*, 15 January 2009. Available at http://www.foreignpolicyjournal.com/2009/01/15/new-media's-moment-in-mumbai/ (accessed 17 October 2011).

40. Pew Global Attitudes Project, "Public Opinion in Pakistan: Concern About Extremist Threat Slips; America's Image Remains Poor," *Pew Research Center*, 29 July 2010. Available at http://pewresearch.org/pubs/1683/pakistan-opinion-less-concern-extremists-america-image-poor-india-threat-support-harsh-laws (accessed 19 October 2011); Pew Global Attitudes Project, "Support for Campaign Against Extremists Wanes: U.S. Image in Pakistan Falls No Further Following bin Laden Killing," Pew Research Center, 21 June 2011. Available at http://www.pewglobal.org/2011/06/21/u-s-image-in-pakistan-falls-no-further-following-bin-laden-killing/ (accessed 19 October 2011).

41. "Pakistan—Floods—July 2010, Table B: Total Humanitarian Assistance per Donor as of 19 October 2011," *United Nations Office for the Coordination of Humanitarian Affairs*. Available at http://fts.unocha.org/reports/daily/ocha_R24_E15913__1110191604.pdf (accessed 19 October 2011).

42. Shefali Anand, "From Abbottabad, Live-Tweeting the Bin Laden Attack," *The Wall Street Journal*, 2 May 2011. Available at http://blogs.wsj.com/indiarealtime/2011/05/02/from-abbottabad-live-tweeting-the-bin-laden-attack/ (accessed 19 October 2011).

43. Frances Stonor Saunders, *The Cultural Cold War: The CIA and the World of Arts and Letters* (New York: The New Press, 2000).

44. Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence* (Washington, DC: Potomac Books, 2009), p. 85.

45. Brachman, *Global Jihadism*, p. 90.

46. Bruce Hoffman, "Al-Qaeda has a New Strategy. Obama Needs One, Too," *The Washington Post*, 10 January 2010. Available at http://www.washingtonpost.com/wp-dyn/content/article/2010/01/08/AR2010010803555.html (accessed 24 October 2011).

47. Chris Battle, "New Media's Moment in Mumbai," *Foreign Policy Journal*, 15 January 2009. Available at http://www.foreignpolicyjournal.com/2009/01/15/new-media's-moment-in-mumbai/ (accessed 17 October 2011).

48. Suzanne Choney, "Twitter: 250 Million Tweets a Day," MSNBC, 18 October 2011. Available at http://technolog.msnbc.msn.com/_news/2011/10/18/8383840-twitter-250-million-tweets-a-day (accessed 20 October 2011).

49. "Remarks By Doug Naquin—Director, Open Source Center," *CIRA Newsletter* 32(4) (2007), p. 7.

50. Brachman, *Global Jihadism*, p. 150.

51. Frederick P. Hitz, *Why Spy? Espionage in an Age of Uncertainty* (New York: St. Martin's Press, 2008), p. 15.

52. Rid and Hecker, *War 2.0*, p. 14.

53. Allen W. Dulles, *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World* (Guilford, CT: The Lyons Press, 2006), p. 53.

54. Rid and Hecker, *War 2.0*, p. 32.

55. Dulles, *The Craft of Intelligence*, p. 55.

56. Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996), p. 65.

57. Robert Service, *Stalin: A Biography* (London: Macmillan, 2004), p. 355.

58. Hitz, *Why Spy?*, p. 32.

59. "The 9/11 Commission Report." Available at http://www.911commission.gov/report/911Report.pdf (accessed 7 October 2011).