INSURGENT MEDIA: WEAPONS OF MASS ATTRACTION

A Thesis
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Master of Arts
in Security Studies

By

Holly L. Ghali, M.A.

Washington, DC
November 19, 2010
Copyright 2010 by Holly L. Ghali
All Rights Reserved
# Table of Contents

Introduction 1

New Media  
  What’s So New About Media 2

Insurgents  
  Weapons of War 5  
  Hijacking the Mass Media 7  
  Supply and Demand 10  
  Networks and Hierarchies 12  
  Cheap and Easy 13  
  They Have Skills 15  
  Global Reach 18  
  Reaching Out 20

Militaries  
  …And Media 22  
  Laws 23  
  Cultures 24  
  Structures 27

Conclusion 28

Bibliography 33
“Among the most dangerous things the West introduced...

are the written, audio and video media.” – Jihad Magazine
In 1970, George Habash, the founder of the PFLP (Popular Front for the Liberation of Palestine), declared to an interviewer, “When we hijack a plane it has more effect than if we killed a hundred Israelis in battle…For decades world opinion has been neither for nor against the Palestinians. It simply ignored us. At least the world is talking about us now.”

In 1995 Timothy McVeigh bombed the Alfred P. Murrah Building in Oklahoma City in the morning when children were present because without the 19 dead children, it “would not have gotten the point across to the government. We needed a body count to make our point.” And more recently, Osama bin Laden wrote to Mullah Omar in Afghanistan that, “It is obvious that the media war in this century is one of the strongest methods; in fact, its ratio may reach 90% of the total preparation for the battles.”

INTRODUCTION

The notion that terrorists and insurgents stage dramatic events as a means to attract media exposure is not a new finding. What is new, is the types of access and ease with which these sub-state groups increasingly use new media to reach out to a mass audience in waging their battles. Conventional militaries have traditionally maintained a monopoly over mass media, barring the rare dramatic event staged by a terrorist along the lines of those referenced above. Rapid innovation and advances in new media technologies have eliminated this monopoly by empowering sub-state actors—and any individual, for that matter—with the ability to instantaneously access a mass audience.

---

3 Document #: AFGP-2002-600321 Full Translation Date: June 5, 2002
In the present political and military environment, terrorists and insurgents use the media, especially new media, as a powerful adjunct to violent action. The plethora of social networking sites, email, and websites also facilitate communication, fundraising, recruitment, and the ability to distribute insurgent propaganda directly to their audience.\(^4\) Terrorists (or insurgents using terrorist tactics) fight conventional militaries with unconventional methods because they are, by definition, too weak to fight them in conventional battles.\(^5\) Therefore, the fight becomes a struggle for public support. Each side, insurgency and counterinsurgency, contends to shape both the attitudes and perceptions of the public, both at home and abroad. An insurgent needs the local population to at least tacitly accept their insurgency, while working to undermine the counterinsurgent’s domestic public support in order to force the counterinsurgent to withdraw from the battlefield prematurely. In the present political and military environment, this battle is fought out in the media.

**NEW MEDIA**

**WHAT’S SO NEW?**

Terrorist groups in the past have used media to promote their causes. Some examples include the clandestine radio stations, underground newspapers, and flyers of the FMLN (Farabundo Marti Liberation Front) in El Salvador, and of the Contras (Nicaraguan Democratic Front) in Nicaragua. But these methods of communication

---


\(^5\) I will be using the terms “terrorist” and “insurgent” interchangeably with the implication that I am referring to insurgents or terrorists who use terrorist tactics.
suffered from poor production quality and limited distribution. Before long, terrorists figured out how to stage dramatic events in order to attract the attention of mass media. The distinguishing characteristic of media warfare today is the information revolution and the rise of new media technologies. The information revolution refers to the dramatic changes taking place during the last half of the 20th century (and the Industrial Revolution) in which service jobs are more common than jobs in manufacturing or agriculture. The accompanying trend toward rapid growth of ever newer and cheaper electronic technologies for communication and the emergence or development of decentralized networks on which they operate has fundamentally changed the way we do things. New media can be considered any capability that empowers a broad range of actors (individuals through nation-states) to create and disseminate real time or near-real time information with the ability to affect a broad (regional or worldwide) audience. These innovations have changed the battlefield, creating a combat zone more conducive to insurgency networks than hierarchical militaries. David Kilcullen, explains the fundamental challenge with respect to the Internet and its benefits to insurgents.

Classical [counterinsurgency] theory deals with “active” and “passive” sanctuaries, methods to quarantine such sanctuaries and their effects on insurgent performance (ie. geographical space) but the Internet provides a sanctuary beyond the current reach of most government capabilities and its effects pose formidable obstacles to quarantine.

While Kilcullen explains the Internet as a sanctuary for insurgents, John Arquilla and David Ronfeldt (1998) go further to illuminate the challenges the Internet (and

---

7 Ibid., p. 194.
information technology in general) pose to institutions. The authors define “netwar” as “societal-level ideational conflicts waged in part through Internetted (sic) modes of communication [where] hierarchies have difficulty fighting networks.”\textsuperscript{10} The networked organizations of insurgents, therefore, gain disproportionate advantage from the Internet compared to hierarchical militaries.

Bruce Hoffman (2006), Gabriel Weimann (2006), and Rid and Hecker (2009) all discuss the emergence of new methods of propaganda and the disproportionate advantages that new media technologies present to insurgents and terrorists. Classical counterinsurgency theory finds two fundamental principals of fighting insurgents. These are, “understand[ing] in detail what drives the conflict in any given area or with any given population group” and the need to “act with respect for local people” (Kilcullen: 2010, 3-4). Robin Anderson (2006) goes to great lengths to illuminate that no military can succeed at – or in fact even conduct – a war without media. So counterinsurgent theory seems to have left something out. Media is an important aspect of any war and modern insurgent movements have learned a few lessons from state-operated propaganda campaigns.\textsuperscript{11} Today’s insurgents have applied these lessons to harness mass media by sophisticated and adaptive uses of new media technologies. Their propaganda moves through mass media—once unavailable to sub-state insurgent groups—via tried and true methods of psychological warfare. In order to do this, insurgents make use of a number of new media technologies: web sites, e-mail, chat rooms, e-groups, forums, online magazines, virtual message boards, and online manuals and guidebooks.\textsuperscript{12}

\textsuperscript{10} Arquilla & Ronfeldt, “Cyberwar is Coming!” (Rand, 1993), p. 5.
\textsuperscript{11} Weimann, Terror on the Internet: p. 6.
\textsuperscript{12} Ibid., p. 7.
Some things limit the access insurgents have to leverage new media against conventional mass media, but this brings to the fore issues of free speech and freedom of the press. Monitoring techniques, including “sniffers” along the lines of Carnivore, Magic Lantern, and Echelon scan the Internet and alert authorities when something of interest triggers the alarm. While these efforts have been helpful, others, including removal of websites, do very little to impede insurgents from sending their messages. New media technology means that the ability to access, collect and convey a message has become decentralized, and the capability to carry out these acts increases exponentially as time passes. This means that militaries need to improve their information warfare tactics and strategies in every aspect of the wars in which they engage.

INSURGENTS

WEAPONS OF WAR

Insurgents face a dilemma about how to account for their inferiority vis-à-vis the state authority or military with which they take issue. Early communist leaders tried to rally support of the masses for a proletarian revolution, while Mao Tse-Tung (1965: 150) emphasized innovation through the development of peasants into the “true bastion of iron.” Succeeding insurgent leaders seized on these inherent qualities of their positions. T.E. Lawrence (aka Lawrence of Arabia) wrote proudly of his adventures in blowing up Turkish railways and Abu Musab al-Suri, (one of Al Qaeda’s strategic masterminds) was


enamored with fellow underdogs Mao, Che Guevara, and Vo Nguyen Giap, referring to them as “the greatest theoreticians in military art.” Thus, innovation and the need for mass support constitute fundamental qualities of any insurgent movement. It is no surprise, therefore, that today’s insurgent movements seek the most innovative way to reach the widest possible audience in their search for support.

Tactical innovation is, as Rid and Hecker (2009: 125) point out, “a necessary condition for all irregulars, whatever their objective. Without tactical innovation, insurrectionists are doomed to be defeated by regular armies.” Gabriel Weimann (2006) equates the new age of terrorism ushered in after the September 11, 2001 attacks with the new age of the Internet. The fact that Al Qaeda terrorists used the Internet to purchase their airline tickets, steal social security numbers, and obtain fake drivers’ licenses only skims the surface of how today’s insurgent movements and terrorist groups make use of new media technology to perform their operations.

---

HIJACKING THE MASS MEDIA

Militaries used to have control of mass media, but insurgents have apprehended that control for themselves by using new media to hijack mass media.

One way that insurgencies make use of new media is to create events that will draw mass media attention to the product. Insurgent terrorist attacks and bombings must be understood as carefully orchestrated media events. The purpose of the event is not the destruction itself, but the effect that the destruction will have on the viewing audience. Insurgencies use violence as a means to attract attention to their cause; in turn, through the attention and publicity this generates, they convey their propaganda. Thus, the violence and destruction are simply a means to bring about the goal of creating a psychological effect (terror), which will not affect those killed in the attack. Actual deaths are simultaneously both necessary and collateral damage. Terrorists began targeting international audiences by staging mass media events in 1968. The first such event was the hijacking of an Israeli El Al commercial flight by the Popular Front for the
Liberation of Palestine (PFLP). A more contemporary example was the attacks in Mumbai by Lashkar-e-Taiba. The operation that killed 166 people used Google Earth to gather intelligence about the buildings and then monitored mass media coverage of the events as they unfolded. The media also monitored and reported on twitter messages as they were being sent out from private citizens at the scene. These messages provided valuable intelligence to the attackers and their Pakistani dispatchers, which they used to make decisions about how to move forward with the plan. The commanders then used cell phones to communicate between Pakistani commanders and the attackers in Mumbai instructing them about how to proceed. The operators called various attackers directing them in how to fight and when to explode hand grenades and set fires in order to have the media to film the destruction. Indian authorities recorded the conversation between an operator in Pakistan and his minions in India. The emphasis on media coverage is evident in the tapes:

Pakistani Operator: “You haven’t set them on fire?”
The attacker: “You’ll notice fire in a moment.”
“Okay, we’ll wait to see it.”
“Listen the two brothers have gone to the sea-facing side to open the door…once it’s open, we’ll set it on fire.”
“Okay, set it on fire…don’t waste time.”
“We have only one room. If we set that on fire, we won’t have a room (laughing).”
“Okay, you’re on the top floor? Go to the other side and set the carpets and curtains on fire.”

“Yes, we will do that once the brothers return.”
“You’ll be late…you haven’t even thrown a grenade. How long does it take to fling a grenade? There are lots of cars parked downstairs.”
“I’m sending them both repeatedly, but they simply don’t throw grenades. They just return without doing it. I don’t know what they’re doing. They say they’re going to throw, but they don’t.”
“What’s the big deal in throwing a grenade? Pull the pin and throw, that’s it…Answer the phone when I call. Don’t spend too much time setting the place on fire.”¹⁹

While the attackers moved around the city, their Pakistani handlers watched news that covered the event to provide further instructions for the ongoing operation. At one time, the operator in Pakistan informed the terrorist of commandos invading the building and instructed them to “fight in the open…the snipers are in position and they will fire at you the moment they see you…the top floor is being cleared by 15 heliborne commandos…”²⁰ The attacks were planned well in advance using the Internet and other methods to gather intelligence. Once under way, the terrorists used cell phones to coordinate the attacks in order to maximize media attention, and the mass media played right into the attackers’ hands by providing the attackers with information about police countermeasures and by providing the force multiplier effect so desired by insurgents.

Communication is central to the insurgent’s ability to convey a message to the target audience. An insurgent will stage a terrorist attack to attract media coverage in the same way that political strategist will stage a media event to garner free news coverage. And media outlets will cover the events for the same reason in both cases: they need content that deals with the issues affecting their audiences. Al Qaeda in Iraq presents another example of how insurgents provide this content. The group made use of media

labs to produce, edit, finalize and compress videos on computers unconnected to the
Internet. The videos were then downloaded to thumb drives or portable hard drives and
taken elsewhere where they could be uploaded to the Internet. A 2007 seizure of the
contents of eight such labs yielded 23 terabytes of material awaiting web distribution.
According to the Multi-National Force-Iraq, this seizure degraded the group’s ability to
recruit via the Internet by 80 percent because the videos served such a significant
propaganda role.21

SUPPLY AND DEMAND

In the case of war, a primary challenge for media outlets is obtaining coverage of
combat operations. Financial constraints, logistics, deadlines, and not least of all safety,
present formidable obstacles to providing coverage for the ever-demanding news cycle.
Insurgent propaganda aimed at recruiting sympathizers to the cause sometimes serves the
dual purpose of providing media content to coverage-starved war reporters. In 2006 The
New York Times Magazine reporter Elizabeth Rubin circumvented the problems of access
by describing videos found in local markets of Kabul, Kandahar, and Quetta.

One begins with clattering Chinooks disgorging American soldiers into the desert.
Then we see the new Afghan government onstage, focusing in on the Northern
Alliance warlords—Abdul Rashid Dostum, Burhanuddin Rabbani, Karim
Khalili, Muhammad Fahim, Ismail Khan, Abdul Sayyaf. It cuts to American
soldiers doing push-ups and pinpointing targets on maps; next it shows bombs the
size of bathtubs dropping from planes and missiles emblazoned with “Royal
Navy” rocketing through the sky; then it moves to hospital beds and wounded
children. Message: America and Britain brought back the warlords and bombed
your children.22

21 Cori E. Dauber, “Youtube War: Fighting in a World of Cameras in Every Cell Phone
and Photoshop on Every Computer,” Strategic Studies Institute, USArmy War College,
By doing this, she effectively transported the videos and their propaganda to her own audience, providing ever more exposure for the video producers.

With new media technologies, insurgents also stage attacks, record them, transfer the footage and post it on the Internet making it available for anyone to download and redistribute. The constraints placed on media outlets and the ease of access to insurgent attack footage via the Internet makes using the material as a news source tempting for mass media outlets.23 Thus, the insurgents provide dramatic content to media outlets, which face formidable challenges to obtaining it through other means, and thereby the mass media is co-opted in spreading insurgent propaganda.

Very little is more dramatic at present time than the videos and audio recordings of Osama bin Laden and Ayman al Zawahiri.24 After the tapes are either delivered to a television station or distributed online mainstream media immediately pick up the story and report their contents. For example, a search on the Fox News website for “Bin Laden Tape” returns 16,665 results.25 These include direct links to the bin Laden videos as well as references to other outlets that covered the subject, including European and Middle Eastern news agencies.26 A search for “jihad video” of the CNN website returns 459 results and includes links to a story titled, “Jihadist website: One of Hamburg terror

---


26 Ibid.
group killed in drone strike.” The author directly transmits information from a blog stating, “A jihadist from Hamburg suspected of being part of an al Qaeda plot against Europe was killed by a drone strike in northwest Pakistan this week, according to a statement Thursday on a Turkish-language jihadist website.”\(^{27}\) Another link reports that, “Al Qaeda No. 2 Speaks on Gaza Flotilla Incident.”\(^{28}\)

**NETWORKS AND HIERARCHIES**

The nature of new media is also more advantageous to insurgencies than to counterinsurgencies because of the structural formation of the adversaries in question. Arquilla and Ronfeldt (2001) explain how the information revolution, “disrupts and erodes the hierarchies… redistributing power, often to the benefit of what may be considered weaker, smaller actors… Meanwhile, the very changes that trouble institutions—the erosion of hierarchy, etc.—favor the rise of multi-organizational networks.”\(^{29}\) They go on to explain characteristics of new media technologies that play directly into COIN operations today.

First, the information revolution is favoring and strengthening network forms of organization, while simultaneously making life difficult for old hierarchical forms. The rise of networks—especially “all-channel” networks, in which every node is connected to every other node—means that power is migrating to nonstate actors, who are able to organize into sprawling multi-organizational networks more readily than traditional, hierarchical, state actors can. This means that conflicts will increasingly be waged by “networks,” perhaps more than by “hierarchies.” It also means that whoever masters the network form stands to gain major advantages. Second, as the information revolution deepens, conflicts increasingly depend on information and communication matters. Conflicts will revolve less around the use of raw power than of “soft power”—


\(^{28}\) Ibid.

\(^{29}\) Arquilla & Ronfeldt, “Cyberwar is Coming!” p. 4-5.
that is, media-oriented measures that aim to attract rather than coerce.\textsuperscript{30}

This increasing influence of “soft power,” explains Robin Anderson (2006), is why media becomes a force multiplier and might even contribute to additional violence for the purpose of staging media events. It also contributes to the fact that insurgent groups remain successful despite statistically higher numbers of casualties among the population they lobby for support. Rid and Hecker (2006) further explain the dilemma in responding: as violent acts are carried out, broadcast on new media, picked up by mass media, and distributed at record pace, counterinsurgents are forced to gather the information, analyze it, verify it, and then structure a response that remains within the standards of truth and accuracy that is expected of counterinsurgent operations. The reactionary nature of this side of the relationship is further evidence of the difficulties that new media presents to counterinsurgent forces.

\textbf{CHEAP AND EASY}

Even in instances such as the Mumbai and World Trade Center attacks, several gatekeepers sat between the event unfolding and the audience viewer. The reporter, the editor, the producer, and possibly even the network executives all weighed in on how much coverage was shown and in which light the event would be portrayed. With the rise of new media technologies, al Qaeda commanders are able to shoot a video on a portable camera, edit it on a laptop, and burn it to a CD or upload it directly to the Internet with little more than a few hundred dollars and an Internet connection. They do this completely free from censorship.

\textsuperscript{30} Ibid., p. 8.
Information technology has become cheaper and easier to use; consequently the superiority once possessed by militaries in terms of resources and power has been equalized by the less expensive accessible technology now available to individual insurgents. As in other industries, the progress in information technology improves the efficiency of the operation’s activities—even routine administrative ones. It has facilitated the ability to conduct various operations, including attacks and training, over long distances. This change essentially minimized the previous need for a large physical presence. Also, because of the portable and facilitative nature of new media technologies, the “central” core of a group can consist of as little as a single commander, a cell phone, and maybe a few bodyguards. This aspect makes the group highly mobile and difficult to locate and attack. As pointed out by Bruce Hoffman, (2006), Osama bin Laden’s pre-recorded message was professionally produced, shot, edited and delivered to Al Jazeera Television to be aired in perfect time with the planned U.S. airstrikes on Afghanistan. The fact that the Saudi billionaire used easily obtainable, cheap, high quality video equipment to appropriate a mass media television outlet is a perfect example of how terrorists and insurgents have combined new media technologies with mass media’s access to the wider world audience.

If to Mao “the important thing is to be good at learning,” the importance of new media technologies to today’s insurgent movements cannot be overstated. As pointed out by Bruce Hoffman, (2006), Osama bin Laden’s pre-recorded message was professionally produced, shot, edited and delivered to Al Jazeera Television to be aired in perfect time with the planned U.S. airstrikes on Afghanistan. The fact that the Saudi billionaire used easily obtainable, cheap, high quality video equipment to appropriate a mass media television outlet is a perfect example of how terrorists and insurgents have combined new media technologies with mass media’s access to the wider world audience.

and its need to fill air time. The return for value that al Qaeda receives on videos is apparently quite good. In 2007, al Sahab, the media arm of al Qaeda, released a record 74 videos, averaging one video every three days (double that of the previous year) and a record number of video releases at the time. The videos along the lines of those described in Elizabeth Rubin’s *New York Times Magazine* article and found in markets in Afghanistan serves as another example of how insurgents there are making the most of the low production overhead of new media.

The World Wide Web is another means by which insurgents have innovated. Benedict Anderson’s (1991) sense of an imagined community has been drawn together at a faster pace, in a more ubiquitous, and inexpensive way than ever. The speed element of the World Wide Web serves insurgent groups, their sympathizers, or radicalized lone individuals significantly. The rapid rate of communication makes government censorship difficult, anonymity powerful, and transmitting propaganda utterly affordable. The fact that these technologies are so adaptable to insurgents who wish to be more innovative is only one aspect of the issue.

**THEY HAVE SKILLS**

One thing that an analyst will quickly discover about insurgent media uses is the core, common characteristics that a majority of them share. A brief survey of insurgent websites demonstrates selective presentation of information in a well designed, colorful and visually pleasing way. Each of the websites contains a description of the group’s history, the aims of the group, biographies of group leaders and news stories selected that

---


34 Rubin, “In the Land of the Taliban.”
often include statements by the leaders or other important members to clarify the group’s ideological beliefs. Monotheism and Jihad’s website features quick links to “39 ways to serve and participate in the jihad,” and links to buy books, read articles, and research interviews on its website.³⁵

Islamic Army in Iraq catalogues videos of attacks perpetrated by its members against coalition forces for web users to watch, and features flashing links to partner websites, “most read” articles, “selected pictures,” and two links to the al Fursan Jihad Magazine, which is published by the Islamic Army in Iraq’s “Central Media Department.”³⁶

Al Qaeda even has a Facebook page, with over 200 “friends” from all over the world. It serves as an efficient way to post news of events and news releases with links to videos, “likes,” and images of other jihadis.

Jarrett Brachman, “Al Qaeda Wants to be Friends,” Foreign Policy website.  

37 Jarrett Brachman, “Al Qaeda Wants to be Friends,” Foreign Policy website Retrieved
GLOBAL REACH

Through the use of new media technologies, insurgents achieve a global reach by recruiting through the Internet, making prohibition of their activities extremely difficult. It is difficult to underestimate the recruitment potential of the Internet. From martyrdom videos distributed in Israel / Palestine to issuing erroneous fatwas condoning wanton bloodshed and violence, the Internet is the primary recruitment tool for insurgents and terrorists.\textsuperscript{38} In Iraq and Afghanistan insurgents have staged events with the aim of filming them and distributing the footage. The videos serve the dual purpose of providing shocking content while simultaneously demonstrating how random and damaging violence takes place under the ostensible protection of counterinsurgent forces. Violence furthers the insurgent cause by proving that the counterinsurgent is failing to provide stability and security.

Cheap video and editing equipment combined with simple reproduction capabilities makes video a valuable recruitment tool. Posthumous videos show suicide bombers explaining their reasoning for their upcoming decision, and videos abound that pay homage to the dead “heroes” of the movement. These combine photos of the “martyr,” snapshots or footage of the attack, if available, and dramatic music and lyrics praising the dead attacker and their cause.

A quick survey of the variety of languages served by jihadist websites makes clear the global nature of this insurgent movement. Some sites include translations or

\footnotesize

\textsuperscript{38} A fatwa is an Islamic religious ruling, a scholarly opinion on a matter of Islamic law.
websites in several languages. Baghdad Sniper’s website, for example, uses dramatic photography and offers its message in English, Arabic, French, Spanish, Italian, German, Turkish, Urdu, and Chinese.\textsuperscript{39}

Insurgents also make use of the Internet for recruiting (using information gleaned from online surveys) and data mining. While this information might be available through traditional means, the Net allows for cheap, instantaneous, and anonymous collection and searching.\textsuperscript{40}

Videos are also used to recruit by providing training in activities such as explosives training and weapons. Jihadi websites feature links to instructions on how to design suicide vests as well as how to assemble an array of other weapons.\textsuperscript{41}

\textsuperscript{39} Baghdad Sniper website, retrieved November 4, 2010 \url{http://baghdadsniper.net/}
\textsuperscript{40} Websites surveyed here include: Minbar al-Tawḥīd wal Jihād \url{http://www.tawhed.ws/}; Al-Būrāq \url{http://www.al-amanh.net/vb/index.php}; Al-İeşh al-İ Arabî fee al-Iraq \url{http://iaisite.org/}; Fursân al-Ḥaq \url{http://www.forsanelhaq.com}.
\textsuperscript{41} “Al Qaeda Online: Understanding Jihadist Internet Infrastructure;” see also “Terrorist Use of the Internet,” both Retrieved November 12, 2010 at Jane’s \textit{Terrorism and Security Monitor} (JHS Global Limited 2010) Retrieved on November 1, 2010 at \url{http://0-}
visual training aids might serve as an instructive tool, but more likely they instill in the viewer the sense that the jihad is something that he can do for himself. Most of them, including the one below, feature the intended effect of the explosives for which training is offered.

**REACHING OUT**

![Image](www.baghdadsniper.net)

Insurgents also use videos as a means of communication. From January 2009 to July 2010 Al Qaeda issued 108 statements and other significant public communications. With the increasing pace of communications and corresponding increase in terrorist attacks some analysts link these messages with subsequent attacks. For example, Peter Bergen points out three statement-and-attack sequences to illustrate the way bin Laden uses media to communicate orders: an October 2003 statement issued by bin Laden denouncing Spain and the subsequent Madrid bombings six months later; the truce

---

[jitic.janes.com.library.lausys.georgetown.edu/IDIC/ITIC/home.do](http://www.jitic.janes.com.library.lausys.georgetown.edu/IDIC/ITIC/home.do)

offered to European countries by bin Laden in Spring of 2004 and the London bombings one year after the expiration of the truce; and the call for attacks against Saudi oil facilities issued by bin Laden late in 2004 followed by the attack on the Abqaiq plant slightly one year later. Oftentimes, after an attack, leaders of one group will issue a video to claim responsibility for carrying out the attack or to inform others of their territorial gains. Other instances of signaling in videos are the various announcements by Ayman al Zawahiri and Osama Bin Laden that they recognize the actions of a group. A recent example includes an audio recording of Mustafa Abu al-Yazid who announced the formation of Al Qaeda in Kashmir. The announcement also claimed an attack that killed 17 people in India, representing an effort to reach out to the Lashkar-e-Taiba networks that have operated in India for some time. The notion of several groups operating together through a few individuals is common. But the recent case of the Mumbai attacks indicates that individuals also operate for several different groups at a time. David Headley was an American-born Pakistani who conducted reconnaissance for the attacks in India and held contacts with Al Qaeda, Harakat al Jihad, and Lashkar-e-Taiba.

New media technologies also go a long way in allowing groups to communicate with their sympathizers and raise funds. Web sites, e-mail, chat rooms, e-groups, forums, online magazines, and virtual message boards all allow real-time interaction for insurgents and sympathizers (or potential sympathizers) to communicate with one another. Many websites publish documents on strategic thought along with their calls for

---

jihad and the applicable lines from the Quran and relevant fatwas.\textsuperscript{46} They also use these channels to further spread their propaganda. As Daniel Byman points out, “sympathetic states, front groups, ideological sympathizers, and diaspora members can serve as transmission belts for insurgent propaganda.”\textsuperscript{47} Diaspora communities have played formidable roles in continuing the resistance of several strong insurgencies.\textsuperscript{48}

Insurgents have also capitalized on the Internet to conduct fundraising. Groups reach out to diaspora communities to collect financial resources. A common way to do this is through charities and religious groups.\textsuperscript{49} In many cases, the donor does not know that the funds will be used for an insurgency and believe that they are helping the poor, the children, or the refugees of their associated group.

\textbf{MILITARIES}

...AND THE MEDIA

Militaries have cultural, structural, and political constraints that prohibit them from adapting effectively to the problems posed by new media. Specifically, the U.S. military has traditionally dealt with the “demands” of the press as a nuisance. Despite fairly recent efforts to change that attitude, interactions between the press and the military remain strained, to say nothing of the failure of the military to coopt the media for its

\begin{flushright}
\textsuperscript{48}Ibid., Intro.
\end{flushright}
cause. Several structural issues challenge U.S. counterinsurgency efforts with respect to new media, among them: the U.S. military’s ability to use the Internet is checked by the Smith-Mundt Act of 1948; the current U.S. Information Operations (IO) strategy is fundamentally flawed; and the U.S. IO is not consistent or coordinated across each of the services, and therefore it is ineffective. Apart from these issues, bureaucratic struggles between the State Department and the Department of Defense over authority for IO implementation and policy direction further hinders U.S. efforts.

LAWS

Foremost among the institutional constraints against the military is a legal one. The military conducts WHITE and Gray Psychological Operations (PSYOPS) on foreign targets. White PSYOPS BLACK PSYOPS are very limited, if done at all. The Smith-Mundt Act of 1948 imposed legal constraints that prohibit the military from conducting any type of PSYOPS on any U.S. citizen anywhere. Many host nations have a similar attitude in terms of the U.S. military conducting PSYOPS operations on their own citizens. This is understandable for many reasons, particularly as this would enable access of a foreign entity (the US) across a spectrum of government and social networks.

Another mission constraint on current counterinsurgency operations is that the fight is ultimately centered on insurgent operatives in many countries where the U.S. is not engaged in combat operations. For instance, despite the suspicion that Al Qaeda is taking refuge in Pakistan, the military is prohibited from applying any COIN strategy in the area, since the U.S. is not currently at war with Pakistan. No development of

---

military doctrinal, legal, or cultural changes would facilitate addressing the problem we face of countering Al Qaeda’s propaganda in Pakistan. With these limits, the U.S. military focuses not so much on the recruiting and indoctrination phase of COIN, but to get information out in places where there is little news in general. This is to counter the insurgent’s mis/disinformation campaigns at the macro level. As the U.S. military has lately operated where there is little Internet, its basic operational approach is geared to what would be considered old media.

CULTURES

As tweeting becomes more common in places like Africa and the Middle East, where more social networking takes place via cell phone, the COIN militaries will be forced to switch to this medium as a means to communicate COIN messages to the population. In this case, the issue is one of switching mediums. This is where a generational issue with the military arises, as it is predominantly the younger generation of officers—thus those with less influence on military operational planning—who understand the technology better than the decision makers. Many in the military chain of command understand this specific aspect of the problem, but addressing this simple issue alone will not make up for the other structural, cultural, and legal challenges the military faces with the use of new media.

Despite the development of Information Operations integrated to employ electronic warfare, computer network operations, PSYOPs, military deception, and operations security across the services, the mission is still facing some challenges. A brief look at the Counter-Insurgency Approach diagram of Information Operations goes a long way to illuminate the convoluted nature of the U.S. military approach to IO in Iraq.
Assuming that the military operators in charge of implementing this mission were able to synchronize the effects illustrated in this diagram—which Maj. Norberto, the author of the article insists they cannot do—the mission is unclear, convoluted, and complicated. Furthermore, this doctrine for IO COIN operations is not coordinated across the services and suffers through lack of effective implementation.\textsuperscript{52}

Traditionally, the military enjoyed most of the control over information in a war zone. Issues of secrecy of operations, planning and targeting instilled the military with an

inherent distrust of media. Over time, this has changed and the U.S. military has made a concerted effort to appropriate the media for its use. Embedded journalists in the beginning of the war in Iraq is a notable example of how the U.S. military has adjusted its relationship to the media. The U.S. Army / Marines Counterinsurgency Field Manual states, “media representatives should be embedded for as long as practicable” to allow the “young people [Soldiers and Marines]” to communicate “the important issues for a broad audience.”53 The traditional resistance to change found in the history of the U.S. military’s approach to mass media, however, seems also to be repeating itself with the military’s approach to new media technologies as well.

Another significant challenge faced by counterinsurgent forces is the willingness of the audience to receive the message. Spreading a message is not possible if the audience is unreceptive. Apparent cultural differences limit the ability of a message’s impact, regardless of the communication tool. In this case, insurgents will be more effective because of their cultural affinities and local knowledge. But how does an insurgent who is responsible for so much death and destruction of a neighborhood convince the local grocer to join his militia? The theory of selective moral disengagement is one potential approach to understanding why individuals are receptive to violent jihadi propaganda. This theory explains that people will generally desist from behavior that is inconsistent with their moral values and will not engage in such conduct until they have justified to themselves that their actions align with their moral values.54

54 This concept as applied to counterterrorism is put forth by Albert Bandura in “The Role of Selective Moral Disengagement in Terrorism and Counterterrorism.” In F.M.
Some components of this selectivity were evident in a brief survey of the websites surveyed. Each of the websites used euphemistic language, the displacement and diffusion of responsibility, and the attribution of blame to portray their groups and events in ways favorable to their causes. This selective moral disengagement then allows them to market their product more effectively because they have what Hoffman describes as effective propaganda material.  

**STRUCTURES**

Apart from the lethargy of the military to harness a rapidly changing technology, when dealing with insurgencies the main question for militaries trying to fight it with IO is whether they must address a large population or the individual. Mass media are traditionally used to reach mass audiences, but some say that recruitment really takes place at the individual level.  

Trying to reach out to individuals in a counterinsurgency operation demands significant resources and often requires inside access to the country’s information network. In COIN, this quickly blurs over into national level intelligence and domestic law enforcement domains of the host country. There is a U.S. cultural aversion for the Department of Defense performing these types of operations not only in the U.S., but even more so overseas. *The 9/11 Commission Report* provides detailed analysis of the obstacles to information sharing across the U.S. domestic government, including the Intelligence Community, the military, the executive branch, and the State

---


Department.\textsuperscript{57} Trying to manage trust and share information is a challenge within our own borders; trying to facilitate those relationships with foreign countries adds immeasurably to the difficulties.

The asymmetrical relationship between insurgents and counterinsurgents plays another important role. The counterinsurgent must maintain a higher standard of honesty and truth, while the insurgent “is judged by what he promises, not by what he does.”\textsuperscript{58} David Galula wrote, “Propaganda is a one sided weapon,” about the disproportionate expectations he observed French colonial Algeria. The existence of violence undermines the control of the security forces and portrays them as powerless in the eyes of the population. Therefore, in violent insurgencies, violence of any kind serves as a demonstration that the counterinsurgent forces are failing.

\textbf{CONCLUSION:}

Cyber-mobilization through the use of new media technologies has fundamentally changed the character of conventional warfare. It poses a formidable challenge to current efforts in Iraq and Afghanistan and it presents the potential to make future wars between nations more likely because non-state actors are forming multinational networks that challenge state sovereignty.\textsuperscript{59} The ease of access and breadth of information on the Internet could increase the likelihood that insurgents and terrorists will acquire

unconventional weapons. The fact that the 2006 London subway plot included chemical explosives that instructions to mix are readily available online serve as proof of this possibility.\(^{60}\)

Serious threats to national security emanate from groups that can and seek to carry out multinational command, which can pull together a variety of groups.\(^ {61}\) A prominent shift in insurgent and terrorist movements today is the increasing number of individuals who travel from their home (or adopted) countries to a foreign nation to acquire training before returning home to commit attacks. Omar Al-Farouk Al Mutalab traveled back to Nigeria before boarding his return flight to the U.S. on which he planned to detonate explosives in his underwear; Najibullah Zazzi went to South Asia to receive training and then returned, planning to attack the New York City subway system; and Faizel Shazad, traveled with the help of family members to Pakistan before returning to the U.S. to attempt to detonate a car bomb in New York City’s Times Square. It is clear that the target audience being fought over is both local and international, which makes the Information Operations goals of the U.S. all the more important.

It might be prudent to point out that many of these groups—Al Qaeda and the Taliban among them—take issue with the West while simultaneously appropriating some of its most characteristic conventions: freedom, innovation, and modernization. Likewise, a dearth of evidence exists that challenges the reported goals of these groups and their actions. The comment in *Jihad Magazine* about the “most dangerous” things introduced

\(^{60}\) The apartment of the attackers was covered in the chemical hexamethalyne triperoxide diamine (HDMT), which requires some skill to make, and is easily ignited by a small spark; but the instructions are readily available online and the ingredients consist of fuel tablets acquired from army surplus stores, hydrogen peroxide, and citric acid.

by the West is only one example of the blatant hypocrisy espoused by some of these
groups. Counterinsurgent efforts should focus on making known this hypocrisy through
the same channels used by the insurgents. Christine Fair and Daniel Byman offer an
example in their *The Atlantic Magazine* article, “The Case for Calling them Nitwits,” in
which they point out the fact that “one in two [suicide bombers] kill only themselves”
and that the image of the pious Taliban simply does not square with the terabytes of
pornography confiscated from them by the ISAF (International Security Assistance
Forces) personnel.”62 But these types of stories could serve the mission well if they were
to be made available on Arabic language websites, through twitter, videos, and print
media in foreign countries as well.

The implication of new media technologies in the hands of insurgents means a good
deal in terms of how it affects militaries. The fact that media technologies are less
expensive and more accessible than they used to be is not what inhibits
counterinsurgency efforts. Militaries are not losing the propaganda war because they
cannot access technology or cannot afford it. Legal restrictions aside, what undergirds
the resistance of militaries to adapt and effectively counter insurgent new media
campaigns is a cultural and structural resistance to change in general. An Improvised
Explosive Device (IED) proposes a tactical challenge to the men on the ground but that
same IED exploding while a man with a video camera looks on can have strategic
implications back in Washington. The very nature of state-sponsored, centralized
militaries means that quick adaptive responses to changing technologies are almost

---

62 Daniel Byman & C. Christine Fair, “The Case For Calling Them Nitwits,” *The Atlantic
Magazine* website, Retrieved on November 14, 2010 at
unheard of. Likewise, the ungoverned nature of the countries where insurgencies exist and the ungoverned nature of the Internet also represent challenges to classical counterinsurgency ideas of “active” and “passive” sanctuaries. Furthermore, once the information is sent out into the world, it becomes a monumental challenge for counterinsurgents to explain or discredit it. This makes it almost impossible for today’s militaries to succeed with the traditional methods of “gain[ing] and maintain[ing] information superiority…”63 The ability of individuals to leverage power with new media in the absence of bureaucratic processes, political or criminal accountability, or ethical standards will always pose a significant challenge to counterinsurgent efforts. In the case of the U.S. military, officials have taken a rather reactive (as opposed to proactive) approach to dealing with the challenges that new media presents to counterinsurgent efforts.

Military planners and leaders grew up in a culture that emphasized war fighting skills and military technology along the lines of “smart bombs” and “unmanned drones.” The ramifications of this are that at the exponential rate that new media technology changes, innovations in military culture are already outdated by the time they are put to paper—much less instilled in the planning process.

Some positive indications of change include “information operations” and “strategic communications” that have each entered the lexicon of military terminology.64 Making use of plans that consider information effects as an outcome of any operation could help

---

64 Department of Defense (DOD) Joint Publication 3-13 provides a doctrinal overview 31 of military information operations. Strategic Communication, as a nascent concept, has no doctrinal underpinnings, but was addressed in a 2008 DOD Quadrennial Defense Review.
to bring some of the planning stages forward. Then allowing a younger generation of officers to implement the operational goals through technologies that they are more comfortable with could further harness some of new media’s technological benefits.

Alternatively, maybe opportunities exist for “outsourcing” the new media aspect of counterinsurgency operations. As the State Department takes on more of a role in areas where we are militarily engaged, the State Department could expand on public diplomacy initiatives and incorporate relevant programs to augment the military / security aspect of the counterinsurgency operations.
BIBLIOGRAPHY


Rid, Thomas, and Marc Hecker. War 2.0: Irregular Warfare in the Information Age (Praeger, 2009).


Weimann, Gabriel. Terror on the Internet: the new arena, the new challenges (USIP, 2006).
