SMALL WARS JOURNAL

smallwarsjournal.com

Winning the Ground Battles but Losing the Information War

Gina Cairns-McFeeters, John Shapiro, Steve Nettleton, Sonya Finley and Daryk Zirkle

Scene Setter

In this era of persistent conflict, the US faces a myriad of challenges—conventional and irregular, with adversaries who increasingly take advantage of the information environment. Fundamentally, we must change our mindset and incorporate the human terrain—and the effects of information warfare—into our operational analysis and planning. While al Qaeda and its adherents try to frame current conflicts as a "clash of civilizations," in reality there is a struggle within Islam to determine the way ahead in the 21st century. Ambassador Holbrooke stated it best: "defining what this war is really about in the minds of the 1 billion Muslims in the world will be of decisive and historic importance."[1] In order to achieve success, we must fully understand the power of information and the requirements for intelligence and influence—both being conducted in competition with the adversary's information campaign that complements their dynamic and flat networked organizations. The information components of counter-insurgency (COIN) strategies are the underlying foundation for all other COIN activities.

Scenario

The year is 2019. The United States has long since withdrawn from Iraq and Afghanistan. Violent extremists maintain a low profile while they fight the "far enemy", the West, preparing for the day when they can safely defeat the "near enemy", local governments, without the threat of intervention from abroad. Their struggle now is waged over the internet, and is going well. In an instant, outreach to disaffected members of Western society has allowed the spread of poisonous ideology, turning the far enemy in on itself. English-speaking jihadists exploit freedom of speech to fund, recruit, train, plan, conduct command and control and routinely execute terrorist acts in the West, despite the best efforts of law enforcement forces mired in legal wrangling. The masterminds behind this strategy leverage every attempt to curtail this activity as evidence of Western corruption, inconsistency, and false principles leading to the decline of Islam. Every "victory" for counter-terror forces is met with simultaneous revenge

[1] Ambassador Richard Holbrooke, as quoted by John Brown. "Strategic Communications and the Graveyard of Empires," posting to the Huffington Post, 29 August 2009, 3:06 PM. http://www.huffingtonpost.com/john-brown/strategic-communications_b_271977.html

attacks in several countries, undermining popular support and bringing the caliphate ever closer to restoration. The information battle continues.

What could have prevented this state of affairs?

The Problem

The scenario presented above is neither far-fetched, nor far removed from reality. The Associated Press reported in November 2009 there are more than 200 websites promoting violent extremist ideology in English.[2] While John Walker Lindh, the infamous American Taliban, had to learn Arabic to become fully radicalized, those who would follow in his footsteps need not invest the time and money, nor even leave home.

Extremist organizations clearly understand the need to communicate their ideas, and have found the information environment—which consists of the internet, as well as satellite TV—to be an effective means to conduct their operations. The information environment is fertile ground for radical ideology and propaganda. Terrorist organizations not only use it to proselytize extremist religious views, spread their version of victory, host training material, recruit future terrorists and gather sympathy for their causes, but their messages are also aimed at undermining the U.S. and its progress in the Iraq and Afghanistan wars.

Extremist websites remain dynamic and prolific. Many of their websites reside on servers located in the United States; others are located in allied and partner nations. Their format and messages are as varied as their groups that use them and the people they attract. Some sites are closed access and tightly controlled avenues of communication, allowing for more operational security. Others are forum driven, soliciting viewers and drawing in the disaffected to post their thoughts, creating an environment where extremists can share tactics, ideas and lessons learned and a repository of training materials and radical ideologies. A third type of site focuses on one-way dissemination, focusing on specific terrorists or extremist groups. Their one-way messaging is composed of insurgent propaganda and blatant advertisement of extremist actions.

Historically, the most popular extremist websites were written in Arabic, but Saudi Arabia reports the number has dropped significantly since 2002.[3] Among these sites, language and dialect can vary widely, limiting their reach. By shifting to English, extremists know they can reach a wide audience, and increase the probability of provoking a disproportionate response from Western governments and media.

With the help of credible messengers and the willingness to translate material into English and other Western languages, the terrorists' messages are gaining traction across a wider audience.[4] English language radical websites now have a firm foothold in the extremist internet environment. These websites target worldwide English speaking audiences in an effort to gain support and recruits for their causes. Extremists are also gaining 'ground' on gaming sites, such

[2] Donna Abu-Nasr and Lee Keath. "200 Web sites spread al-Qaeda's message in English," Associated Press, 20 November 2009.
[3] Ibid.
[4] Ibid.

as Second Life. They use this 'underground' environment to funnel money, recruit and distribute command and control messages.

A broad audience is important to extremists because, as Ayman al-Zawahiri acknowledged in 2005: "In the absence of…popular support, the mujahed movement would be crushed in the shadows."[5] Only by spreading their message far and wide can extremists hope to build sufficient passive support in which to "swim." While passive supporters do not commit violence themselves, they are often in the position of knowing enough to thwart terrorist attacks, if they choose. A recent bombing investigation in Istanbul estimated there were 200 passive supporters per bomber.[6] Passive supporters present a special problem to law enforcement because they do not actually commit a prosecutable crime. Extremists and their active facilitators, while easier to prosecute, are not persuadable. They demonstrate their commitment through their acts. The combination of extremist commitment and necessity of passive support make passive supporters the object of the "hearts and minds" battle. Not only are adults the desired object of influence, but there is a big push to attract a much younger audience in order to prepare the next generation to carry on their cause. Extremist cartoons and videos appealing to children are becoming more popular. If the extremists' messages are the first to be heard and start to resonate with the young and impressionable audiences, it has already taken hold and the U.S. is starting from a disadvantage.

In this context, Field Marshal Templer's original sense of "hearts and minds"[7] is valuable. "Hearts" refers to convincing potential supporters that extremists' goals are in their best interest.[8] This is the reason behind the plethora of extremist religious and Sharia law arguments on the internet: they establish the common ground necessary to build the perception of a "better life" for Muslims under extremist rule. With this basis, extremists must win "minds" by convincing the audience they can actually win, and secure a permanent change.[9] Terrorist tutorials and online training simultaneously reduce the chance of being caught and imprisoned by authorities and increase the potential pool of recruits. Publicizing successful attacks demonstrates the vulnerability of U.S. forces, and erodes the American will to remain engaged in a distant conflict. Within this context, the internet is a low cost/high payoff tool for extremists. The extremists have nothing to lose and their return on investment is great.

The internet is an easily accessible, low cost/low entry, unbounded environment, with no single ownership or nationality requiring regulations or constraints. Virtual anonymity provides the ability to conduct command and control and funding operations while hiding in plain sight on gaming websites and online forums. In an instant, our adversaries can reach a worldwide network of terrorists, potential terrorists and terrorist sympathizers with their emotionally

---

[5] U.S. Department of Defense, *Quadrennial Defense Review Report*. Washington, DC: Government Printing Office, 2006. p. 23.

[6] Edmund F. McGarrell, Joshua D. Freilich, and Steven Chermak. "Intelligence led policing as a framework for responding to terrorism," Journal of Contemporary Criminal Justice, Vol. 23, No.2, 2007, pp. 142-158. Quoted in Christian Leuprecht, Todd Hataley, Sophia Moskalenko and Clark McCauley. "Winning the Battle but Losing the War? Narrative and Counter-Narratives Strategy," Perspectives on Terrorism, Vol. III, Issue 2, August 2009, p. 28

[7] Brian Lapping. *End of Empire*. London: Granada, 1985. p. 224.

[8] Dave Dilegge, posting to Small Wars Journal blog, October 21, 2007, 9:25 AM. http://www.smallwarsjournal.com/blog/2007/10/hearts-and-minds/

[9] Ibid.

compelling arguments to support their cause. Extremist websites are also a virtual alternative to physical training camps. Previously insurgents and terrorists had no choice but to train at camps in Iran, Syria, Afghanistan, and elsewhere. In today's world of ever-emerging technologies, terrorists no longer have to attend training in remote parts of the world—they can do so from their homes.

A final advantage extremists gain from the internet is their lack of constraints and legal impediments compared to the United States government. Terrorist safe havens are no longer limited to geographical boundaries, and have now transitioned to the virtual environment. They use the cyber battle space in almost unchallenged fashion, and maintain the agility and flexibility to avoid prosecution. They do not need to adhere to the truth, constantly justify costs to a skeptical tax-paying public, nor struggle to understand their target audiences. They exploit these advantages ruthlessly to convince populations globally and they are winning.

The advantages extremists derive from operating in the information environment are bolstered by the challenges faced by the United States government. The foremost of these are the long lead time required to gain consensus through our bureaucratic processes and international diplomacy and the requirement to produce information effects on demand. In this society of instant gratification, we are challenged to provide meaningful measures of effectiveness quickly—changing a population's attitudes, opinions and beliefs cannot be achieved overnight, but rather only through years of continuous 'drum beats' of our message, along with supporting actions. Gaining the trust of countries to achieve cooperation is also becoming more difficult, especially those countries where satellite TV broadcasts are being uplinked from—this requires delicate diplomacy in areas where we are often at odds in pursuing global values and views.

Another challenge we face is turning intelligence support for Information Operations (IO) into a more effective resource. The traditional intelligence community is mired in a Cold War mentality of preparing for the ground battle (who/what/where/when/how) vice the cognitive battle (why) and is not optimized to support the dynamic battle being waged in the information environment. The strength of military intelligence is its ability to provide battlefield awareness to combat troops, not cultural, cognitive and contextual data needed to operate in the information environment.

Where We Are

In the face of this extremist effort, the United States' most visible efforts have been the invasions of and subsequent COIN operations in Afghanistan and Iraq. While these operations have met with kinetic successes, Secretary Gates succintly noted "the United States cannot kill or capture its way to victory."[10] In making this statement, Secretary Gates was doing more than referring to the steadily climbing costs, already in excess of $1 trillion.[11] He was outlining the requirement for a whole of government approach to terrorism. Without an integrated, Interagency/whole of

[10] Robert M. Gates. "A Balanced Strategy, Reprogramming the Pentagon for a New Age," Foreign Affairs, January/February 2009.
[11] Amy Belasco. *The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11*. Washington, DC: Congressional Research Service, 2009. p. 8

government approach, to include our International partners and affected governments, we are making it easier for our enemy.

Military operations in Iraq have progressed from successful high intensity combat operations that defeated one of the world's largest armies in three weeks to COIN and stability operations. These latter-day efforts have resulted in thousands of killed or captured insurgents, and significant progress toward a sovereign, secure, stable and self-reliant Iraq that is on the path to becoming a contributor to peace and stability in the region and beyond. But challenges remain and the gains are reversible.

To paraphrase General Odierno, Commanding General Multi-National Forces-Iraq, "although we have made tremendous strides on the ground, it will be for nothing if we allow the enemy to win the information battle." We not only stand to lose hard-gained ground, but also run the risk of losing the overall war—and our global reputation in the process. Extremist groups fully understand they do not have the ability to meet U.S. forces on the physical battlefield, head-to-head. They compensate for this physical incapacity by using readily available and inexpensive Strategic Communications capabilities, especially via the internet, where they unleash an avalanche of extremist messaging from their virtual safe havens. We have not been able to completely and effectively counter the extremists' public information campaigns in terms of quality, quantity and timing of product dissemination. Thus the nation that invented marketing on Madison Avenue is losing the Madison Avenue war in Iraq and Afghanistan because we have failed to understand the 'human terrain' and have not taken the time to listen.

Conducting operations at the necessary speed will also require an institutional shift toward action, along with definitive policy laying out specific authorities, limitations and responsibilities. The requirement was articulated in the 2006 Quadrennial Defense Review as:

- The ability to communicate U.S. actions effectively to multiple audiences, while rapidly countering enemy agitation and propaganda.
- Joint coordination procedures, systems and, when necessary, command and control to plan and conduct complex interagency operations.[12]

To date, the procedures in place have proven too slow to react to agile adversaries, and now that the threat is widening its audience by shifting to English, speed is even more important.

Where We Need to Be

Joint doctrine establishes the principal methods we might employ to affect our adversaries. We must have the authorities, approvals, intelligence support, abilities, and capabilities to employ that doctrine and to provide the Commander on the ground all available tools so he can act quickly inside his area of operations to directly engage our adversary through multiple avenues. The goal is to make the cyberspace domain an untenable place for violent extremist organizations and groups to conduct operations. We must work with our partner organizations to break through bureaucracy and clarify confusion on operations to affect our enemies' ability to

[12] U.S. Department of Defense, *Quadrennial Defense Review Report*. Washington, DC: Government Printing Office, 2006. p. 24.

continue to distribute their global messages and radical ideologies via the internet and media outlets. We must set clear, directive guidelines for DoD and other government organizations so we can cooperatively synchronize operations to affect the enemy while protecting our own resources.

When extremist websites are discussed, computer network operations are commonly the first means considered. As mentioned above, DoD has established military doctrine to conduct IO against our enemies in cyberspace, but extremists are not conventional military targets. This places potential actions in the Interagency realm, as well as the private business sector and the International community. While the U.S. has multiple Interagency teams operating on the physical battlefield, the level of coordination achieved there has not been matched in cyberspace. Until we move beyond Interagency obstacles, biases and cultures, legal impediments, protection of resources and intelligence counter-priorities, these goals cannot be achieved, and we WILL continue to lose the influence fight in the information environment. The USG must force governmental agencies to focus on unity of effort and effective coordination of operations, or be held accountable for obstructing progress in meeting National-level objectives. This effort will require a significant shift toward action as well as the authorities, approvals, abilities, and capabilities to immediately address, dominate and defeat our enemies as they continue to use the virtual battle space at will.

In addition to intra-governmental coordination, we must tap into all available resources within our reach—starting at the grassroots level within the U.S. Muslim diasporas in the U.S. are a rich resource that can assist in getting our message out to the larger Muslim community. American Muslims can help demonstrate how Islamic beliefs do not need to be compromised thereby exhibiting how we draw upon our diverse heritages to form a united strength. This can help counter the radical ideologies positing Islam has lost its path in the modern world and must return to its past or risk decline.

Our Interagency partners working together can address the problem from a USG perspective, but to be globally effective we need to reach out to our partner nations and enhance the Public/Private partnership to combine and synchronize efforts. The USG should play a key role in coordinating this global effort, leveraging international and technology conferences and diplomatic forums to address the global nature of the extremist message campaign that is thriving on the internet.

As we move toward a whole of government solution on extremist websites, and the use of the wider information environment to incite violence, we must keep in mind the dynamic nature of the internet and use that to our strategic advantage. While we conduct operations to reduce the amount of extremist messages, we must also be able to continuously fill the gaps with viable alternatives to the extremist narrative. As reported by the AP, Saudi Arabia has had relative success in directly engaging potential terrorist recruits and offering them a less radical path. Of 2,631 militants engaged by the Saudi program, 1,170 withdrew the support for extremists.[13] An analogous U.S. program would necessarily have to be run by credible constituents. Fortunately, the U.S. has experience in this, as exemplified by the Alliance of Youth Movements discussed by

[13] Donna Abu-Nasr and Lee Keath. "200 Web sites spread al-Qaeda's message in English," Associated Press, 20 November 2009.

former Under Secretary of State for Public Diplomacy and Public Affairs James Glassman in April.[14] This approach requires long term strategic planning, a tolerance of criticism from within the government, and assistance from international partners for maximum effect.

Conclusion

America's involvement in Iraq has been characterized as "winning the battles, losing the war" almost since the beginning. More accurately, we may be winning the ground battles but we are slowly realizing the information war is being lost. In 2008, cyberspace was designated a global domain on a par with land, sea, air and space. Our enemies are winning in the information environment, while we continue to discuss and debate how to operate in this environment. Our adversaries are using simple, cost-effective means to close the physical battle space gap by taking control of the narrative and effectively subverting with their radical ideology and propaganda. It is absolutely critical for every government agency within the U.S. government to participate, coordinate, cooperate, and arrive at a final, integrated and definitive standard of Strategic Communications against terrorists. We must take the lead in shaping discussions at the national level and work through bureaucracy to clear up confusion and set clear, directive guidelines to be able to deny the enemy the ability to achieve victory in cyberspace and maintain freedom of movement to achieve Information Superiority. The war fighting environment is changing and the arsenal is now communications and information systems. Keyboards are becoming the weapons of choice—are we ready to take on the challenge or are we going to cede victory to the enemy because we have not yet finished the debate on how to adapt for future operations?

Captain Gina Cairns-McFeeters, U.S. Navy, was the Chief, Multinational Force-Iraq IO Cell and led Strategic IO efforts for Iraq.

Captain John Shapiro, U.S. Navy, was Multinational-West IO Liaison Officer to the MNF-I IO Cell.

Lieutenant Colonel Steve Nettleton, U.S. Army, was the Officer in Charge, Cyber Support Element – Iraq and provided computer network operations support to MNF-I.

Lieutenant Colonel Sonya Finely, U.S. Army, was the Deputy Director, Commander's Initiative Group, MNF-I and assisted the director of the Commanding General's personal staff.

Lieutenant Commander Daryk Zirkle, U.S. Navy, was the Information Operations Planner, MNF-I IO and provided planning and staff support to Strategic IO efforts.

Additional Resources

Erin K. Fitzgerald and Anthony Cordesman. *Resourcing for Defeat: Critical Failures in Planning, Budgeting, and Resourcing the Afghan and Iraq Wars*, Washington, DC: Center for Strategic and International Studies (CSIS), 28 August 2009.

[14] James Glassman. "Can a Conversation Win the War on Terror?" Address to InfoWarCon, 24 April 2009. Posted to http://www.jameskglassman.com/?p=94 April 29, 2009.

U.S. Department of State, *U.S. Government Counterinsurgency Guide*. Washington, DC: Bureau of Political-Military Affairs. January 2009.

Admiral Michael Mullen. *From the Chairman: Strategic Communications Getting Back to Basics*, *Joint Force Quarterly* Issue 55, 4th Quarter 2009.