Surfing in Riyadh.

AP / Wide World Photos (Kamren Jebreili)

WAR.com

The Internet and Psychological Operations

By ANGELA MARIA LUNGU

Cyberspace *clickskrieg* represents a dramatic shift in strategic thinking that changes the way we look at war. As an information medium and vehicle of influence, the Internet is a powerful tool in open societies as well as others where the only glimpse of the outside world increasingly comes from Web pages, e-mail, and chat rooms. This electronic innovation cuts both ways, as enemies adopt the Internet as a vehicle for influencing public opinion or inciting hostility against the United States. The Armed Forces must be able to wage war online. Consequently, the realm of military psychological operations (PSYOP) must be expanded to include the Internet.

Major Angela Maria Lungu, USA, is assigned to U.S. European Command; she has served twice with 1st Psychological Operations Battalion (Airborne) and was primary author of Field Manual 3-05.30, *Psychological Operations*.

The Information Battlefield

Together with both public diplomacy and military public affairs, psychological operations is an important instrument of national security strategy. While all three elements play a key role in information operations and reinforce each other, they have separate functions and unique missions. Public diplomacy is an interagency effort focused on foreign audiences. Psychological operations uses specific techniques to influence non-U.S. audiences. By contrast, public affairs activities do not "focus on directing or manipulating public actions or opinion" and by law "must be separate and distinct” from psychological operations. Similarly, public affairs cannot be used as military deception or as disinformation for domestic or foreign audiences, nor can “propaganda or publicity designed to sway or direct public opinion . . . be included in [Department of Defense] public affairs programs.”[1]

Because of new technology and global media, there is an increased overlap of information between public affairs and psychological operations. The public affairs mission has shifted from delivering specific products (newspapers and radio/television) to the processing of themes and messages. This refocus makes it crucial that public affairs, psychological operations, and public diplomacy, as well as other elements of information operations, be fully integrated and synchronized. Public information, both domestic and international, must be consistent on all levels to preserve the credibility of each instrument. Although psychological operations, public affairs, and public diplomacy messages may differ, it is critical that they do not contradict one another.

there are international legal barriers to using the Internet for psychological operations

Limits of Mind War

Psychological operations convey selected information to foreign audiences. A key mission is serving as the voice of a supported commander to political decisionmakers, other commanders, forces, and civilian populations, as well as sources of external support, to influence their emotions, motives, and objective reasoning, convey intent, and affect behavior. It is critical that every theme and objective reflect and support national policy, and informational programs must be integrated into all international information programs to ensure consistent, complementary messages.

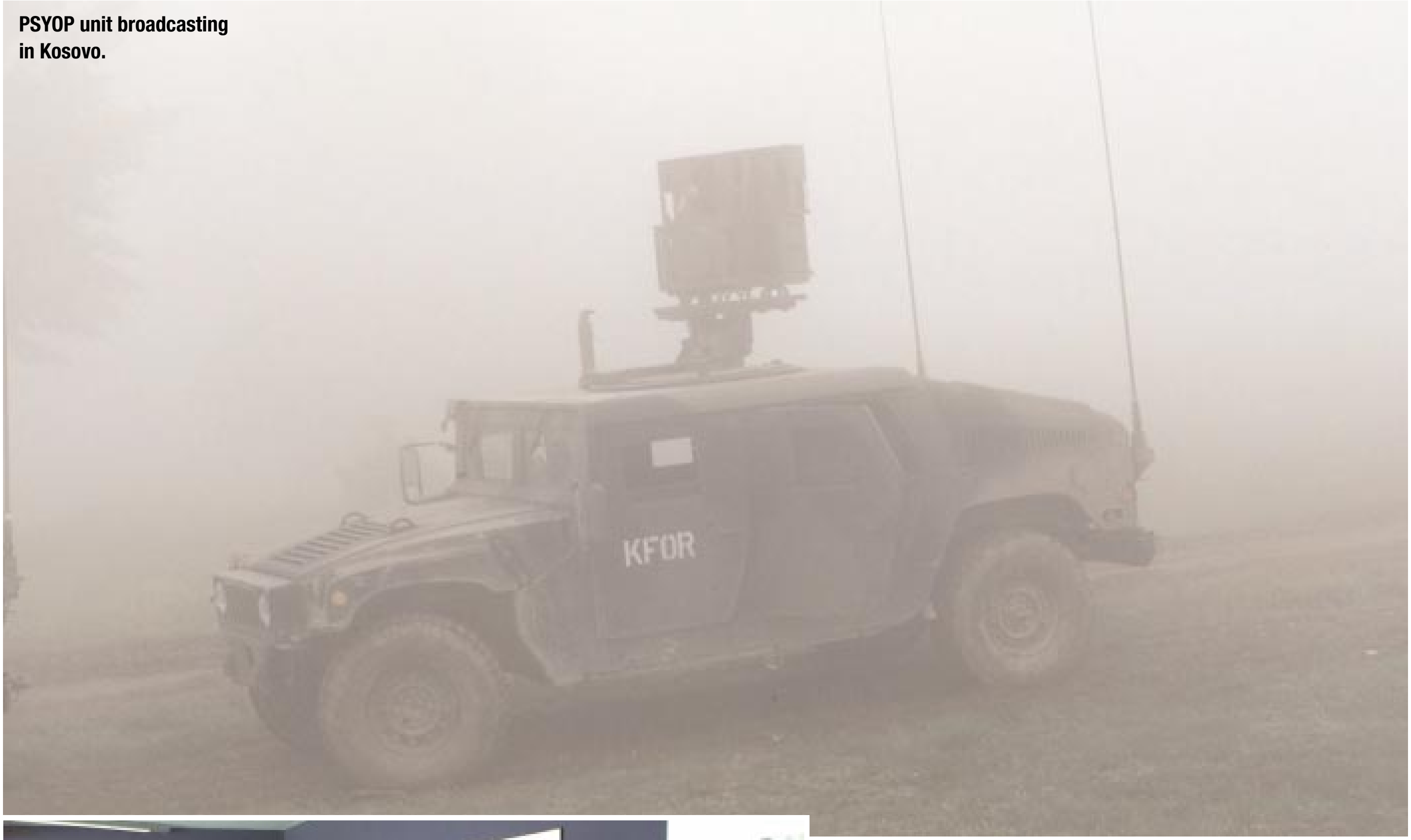
There is renewed interest in using coordinated information programs, in particular military psychological operations, for three compelling reasons. First, there is a politically-driven effort to prevent escalation by a potential enemy toward violent resolution of differences. Second, because of the Internet and other communications technologies, it is almost impossible for governments to regulate the flow of information across their borders, thus making target audiences more accessible to PSYOP messages. Third, the growing world trend toward urbanization, particularly in the third world, makes the use of overwhelming firepower on battlefields brimming with noncombatants far less palatable. Moreover, all these lessons have been learned and applied by potential enemies.

The capability of the Armed Forces to communicate effectively and persuasively with local leaders will be key to achieving both political and military goals. More importantly, in many cases the destructiveness of conventional weapons and limits of diplomacy make non-lethal instruments such as psychological operations useful in filling the gap between diplomacy and force.

But significant legal constraints remain. Laws governing public diplomacy, because many PSYOP products and their dissemination constitute a form of public diplomacy, also control military psychological operations. The Smith-Mundt Act (1948) forms the basic charter for public diplomacy after World War II and established the U.S. Information Agency (USIA). The Foreign Relations Act of 1972 amended the Smith-Mundt Act to ban disseminating any “information about the U.S., its people, and its policies” prepared for dissemination abroad within the United States. The Zorinksy Amendment further restricted public diplomacy by prohibiting that any funds be used “to influence public opinion in the [United States], and no program material . . . shall be distributed within the [United States].” In addition, the Foreign Relations Restructuring Act of 1998 merged several agencies, placing USIA under the Department of State.

The point of contention derives from the difficulty of sending one message to international audiences and another to domestic media, particularly when seen through a legal lens. Presidential Decision Directive 68 focused on this point, stating that international public information activities “are overt and address foreign audiences only,” while noting that domestic information should be “deconflicted” and “synchronized” so as not to send a contradictory message. As one official said, “In the old days, [USIA] and State were the main agencies for communicating internationally. With the information revolution, all agencies now have the ability to communicate internationally and interact with foreign populations.”[2] The directive serves to ensure that these actors are coordinating their efforts.

In addition to domestic limitations, there are international legal barriers to using the Internet for psychological operations. Explicit regulations of particular actions and more general principles of international law may inadvertently constrain PSYOP efforts because information technology is newer than existing laws. This results in both ambiguity in the definition of war and a lack of provisions explicitly prohibiting information attacks. Consequently, areas of contention remain in the realm of information warfare.



PSYOP unit broadcasting in Kosovo.

982d Signal Company (Matthew Siemion)

Internet cafe in Kosovo.

AP/Wide World Photos (Visar Kryeziu)

There are several reasons for difficulty in resolving these issues. Although the perpetrators of cyberwar may be formally organized militaries, netwar attacks may not involve traditional forces. Additionally, it is not clear that information attacks, especially when they are not lethal or physically destructive, constitute the use of force under such provisions as the United Nations Charter and may thus be legal forms of coercion even in peacetime. Conversely, distorting enemy perceptions may be illegal or limited by laws against perfidy.

Despite legal constraints, many areas of psychological operations are considered within the realm of international law. For example, the rules of the International Telecommunication Union do not apply to belligerents, making communications in war fair game. Specifically, manipulating enemy perceptions, spreading confusion by covertly altering official announcements or broadcasts, or frightening leaders by spoofing intelligence or other communications would not violate the laws of war in principle. However, manipulating an enemy until its citizens or leaders became unhinged from reality, or using propaganda, video morphing, or deceptive broadcasts to spur unrestrained civil war or genocide might be considered illegal.

Tactics and Strategies

Given the opportunities afforded by the Internet, and without violating law, there are several options for employing this medium. The Armed Forces could use it offensively to help achieve unconventional warfare objectives as well as to address and counter enemy propaganda, disinformation, and neutral party information.

U.S. Air Force

C–47 dropping leaflets over Vietnam.

The major arguments against Internet PSYOP concern isolation of target audiences, namely preventing Americans from receiving Internet products. Without changing the restrictions against specifically targeting U.S. citizens, however, it is still possible to alter existing policies prohibiting the use of the Internet by military PSYOP. Unintended consequences can be avoided by focusing on disseminating credible information to specific groups. For example, USIA maintained separate Web sites for American citizens and foreign audiences until it was incorporated into the Department of State. Today the English-language Web site of the Office of International Information Programs (formerly USIA) still differs from French and Spanish sites, primarily in that the non-English sites contain links to articles on human rights (specifically on Cuba and Peru), drugs, and corruption, as well as reports on democracy and the AIDS epidemic, none of which appear on the English site. Of particular note is that French and Spanish sites are linked to the Voice of America, which by law cannot be broadcast into the United States.

the major arguments against Internet PSYOP concern isolation of target audiences

There are examples of the potential capabilities of the Internet as a PSYOP medium. State and nonstate actors increasingly turn to the Internet to gain domestic and international support and approval, which helps legitimate the issue for international organizations. As the executive agent for the Dayton Accords, the Organization for Security and Cooperation in Europe (OSCE) used the Internet to complement conventional public information and voter information efforts to reinforce its legitimacy as an international organization.

In addition, the Internet was employed to indirectly distribute information to both local and international media, as noted by the OSCE public information officer in an e-mail to the author:

> *All BiH* [Bosnia and Herzegovina] *media use our webpage to gather information on the OSCE and elections, and in turn distribute it to the BiH public. As well, over 100,000 out-of-country voters, in more than 80 countries, use our webpage as a source of information on the elections—with the OSCE BiH webpage, general election information and election results which would normally be impossible to find is only as far away as their fingertips. In the month leading up to the last election, the OSCE BiH webpage received over two million hits, but the majority of these were from outside of BiH rather than within.*

Beyond simply providing information, Serbs and Kosovars used this technique in what has been described as the first online war in which both sides used Web sites and e-mail to "make their case, to set goals, retell histories, and make stands."[3] As information operations become more popular and refined, it is apparent that instead of a denial of service, information operations should increasingly focus on affecting the perceptions and behavior of selected audiences by manipulating the information available.

After NATO bombed Serb media outlets considered the source of Milosevic's propaganda, for example, the U.S. Government decided not to cut off Serb Internet sites. As the Department of State spokesman observed, "Full and open access to the Internet can only help the Serbian people know the ugly truth about the atrocities and crimes against humanity being perpetrated in Kosovo by the Milosevic regime."[4] Even though the Serbs used the Internet to spread campaign themes, the Department of State countered with a rigorous online effort to defend U.S. credibility. During the Kosovo crisis, the former chief information officer at USIA stated, "the measure of [USIA] success is the extent to which we are perceived not as propaganda but anti-propaganda."[5]

Yet another implication is the changing dynamic that the Internet brings to information war, namely, talking to enemies without the intervention of either governments or propaganda. During the NATO bombing of Serbia, the media and even individuals maintained open communication via e-mail and chat rooms. The international editor of MSNBC.com had an ongoing conversation with three dozen Serbs. The online magazine *Slate* published the diary of a correspondent in Belgrade during this period.

AP / Wide World Photos (Sachai Lalit)

Laotian monks on Web in Vientiane.

The ability of the Internet to forge personal contacts can also be turned into an information advantage. A recent report by the Defense Science Board on psychological operations suggested some less obvious possibilities such as chat rooms and instant messaging services for guided discussions to influence citizens on certain topics and noted that both U.S. presidential candidates and the Chinese government have used similar technology to disseminate information. In addition to Web sites, preempting messages and developing Internet products such as streaming audio/video, online games, mediated news groups, and ad banners can also be leveraged for their strategic value and reach.

Information could also be transmitted over the Internet to sympathetic groups in areas of concern, allowing them to conduct operations in which Special Operations Forces might otherwise be needed to reach target groups. The Internet can also be invaluable for getting news out of the region and into U.S. Government hands, as well as getting information from the United States into a region and cultivating political (and even operational) support. Because journalists may not have access to crisis locations, they might also rely on Internet sites for information, which serves to further multiply the effectiveness of the side able to get its story out.

Kosovo and Chechnya provide examples. Both the Serb government (http://www.serbia-info.com) and Kosovo Liberation Army (http://www.kosova.com) are using Web sites and e-mail to make their cases. The Chechen site (http://kavkaz.org), run by a former information minister, learned from the Serbs and features video footage of Russian bombing and shelling. As a result, Moscow launched the Russian Information Center (http://www.gov.ru). After losing the propaganda war in 1994–96, senior Russian strategists developed a concentrated media plan to target popular support for actions during the second Chechen war.

The Internet can also be employed as a defensive technique, primarily by guarding against defacement of official Web sites and databases. Filtering and blocking software can be installed on individual computers, at an Internet service provider, or on country gateways linking to the rest of the world, and Web sites themselves can block users based on Internet protocol addresses, which can identify particular computers as well as their locations.

The Internet is an inevitable extension of the battlefield, and using it as a critical capability for psychological operations in war is essential. Clearly, a growing number of state and nonstate actors are taking advantage of this tool, given its low cost, particularly in less developed nations. Equally obvious is the need to amend existing policies to allow PSYOP assets to embrace the range of contemporary media. Although current international law restricts many aspects of psychological operations, there is ample legal room for the United States as well as its enemies to conduct psychological operations using modern technology and media such as the Internet.

As the Defense Science Board warned, "while the U.S. is years ahead of its competitors in terms of military technology, in terms of PSYOP there are already competitors on a par with or even arguably more sophisticated than the U.S." Thus the Armed Forces must address the use of the Internet for psychological operations directly and explicitly as an integral asset instead of as an uncontrollable instrument whose role is determined by happenstance or afterthought. JFQ

NOTES

[1] Joint Publication 3-61, *Doctrine for Public Affairs in Joint Operations*, p. III-18; DOD Directive 5122.5, *Public Affairs Program* (February 12, 1993).

[2] Ben Barber, "Group will Battle Propaganda Abroad," *The Washington Times*, July 28, 1999.

[3] Vesna Peric-Zimonjic, "Media-Yugoslavia: Kosovo Combatants Fight New War—In Cyberspace," *World News*, August 7, 1998.

[4] Jon Swartz Briscoe, "Administration Drops Idea of Blocking Serb Net Sites," *The San Francisco Chronicle*, May 15, 1999.

[5] Ibid.