

Influence Operations and the Internet: A 21st Century Issue

Legal, Doctrinal, and Policy Challenges in the Cyber World

*Col Rebecca A. Keller, USAF**

The conduct of information operations (IO) by the US military, which includes military deception (MILDEC) and psychological operations (PSYOP), is based on doctrinal precedence and operational necessity. The increasing use of cybertechnology and the Internet in executing IO missions offers technological advantages while simultaneously being a minefield fraught with legal and cultural challenges. Using Joint and Air Force doctrinal publications, published books, and academic papers, this thesis defines relevant terminology and identifies current operational and legal constraints in the execution of IO using cybertechnology. It concludes with recommended remediation actions to enhance the use of the Internet as a military IO tool in today's cyber world.

Primer on Influence Operations

According to Joint Publication (JP) 3-13, *Information Operations*, IO is "integral to the successful execution of military operations. A key goal of IO is to achieve and maintain information superiority for the US and its allies . . . [in order] to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."¹ Two of the five core capabilities of IO are PSYOP and MILDEC, while Public Affairs (PA) is considered an *IO-related capability*.² All three are inherent in the conduct of military operations from peacetime to wartime and are increasingly affected by cyber-technology. In order to understand these missions, it is important to first explain their definitions and functions.

According to JP 3-13.4, *Military Deception*, short of perfidy, the intent of MILDEC is the execution of actions "to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations."³ Deception has been a recognized component

*Lt Col Michael Masterson, USAF, was the essay advisor for this paper.

of war for millennia; nearly 2,500 years ago, Chinese military strategist Sun Tzu stated “all warfare is based on deception.”⁴ In modern times, two classic examples of military deception are (1) Operation Mincemeat, the World War II deception strategy that convinced the Germans that the Allies were preparing to invade Greece instead of Italy, and (2) a perfectly executed ruse by the Egyptians and Syrians giving the appearance of a military exercise. Instead, they initiated the 1973 Arab-Israeli War, catching the Israelis completely off guard.⁵

While MILDEC is customarily a wartime mission, PSYOP is conducted during all phases of military operations, including peacetime, and is authorized under Title 10, section 167 of the *US Code*, which allows the Department of Defense (DOD) to conduct PSYOP as part of special operations campaigns.⁶ JP 3-13.2, *Psychological Operations*, states the purpose of PSYOP is to influence foreign audience perceptions and behavior as part of approved programs supporting US policy and military objectives.⁷ Since World War I, the United States has released psychological leaflets across enemy lines to persuade and influence behavior. Other traditional forms of PSYOP include ground-based and airborne loudspeaker or radio broadcasts to foreign audiences and show-of-force missions where military ground personnel, aircraft, or ships visibly remind foreign nations of US combat capabilities.

Propaganda is “a form of communication aimed at influencing the attitude of a community toward some cause or position.”⁸ While historically not a pejorative term, the terms *PSYOP* and *propaganda* are often freely interchanged and have taken primarily derogatory connotations. This is in spite of the fact that both provide important national security tools and are truthful in content during the execution of conventional military operations.

Where PSYOP and propaganda are communications directed at foreign audiences, military PA offices provide similar information to journalists and the American public to articulate DOD positions on policies and operations. The same principles based upon the freedom of the press that guide civilian journalists also guide the activities of PA professionals. Military PA responsibilities are captured in JP 3-61, *Public Affairs*—“providing truthful, accurate and timely information . . . to keep the public informed about the military’s missions and operations, countering adversary propaganda, deterring adversary actions, and maintain[ing] trust and confidence of the US population, and our friends and allies.”⁹ Even Pres. Abraham Lincoln understood the importance of interacting with the public, stating, “Public opinion is everything. With it, nothing can fail. Without it, nothing can succeed.”¹⁰

The requirement to influence foreign attitudes and behaviors is not unique to the DOD; the Department of State’s (DOS) public diplo-

macy efforts can often overlap with military PSYOP or PA activities. Out of necessity, DOS public diplomacy and military PA distance themselves from the highly controversial MILDEC, PSYOP, and propaganda mission sets in order to maintain a sense of credibility and operational effectiveness which is “predicated on [the] ability to project truthful information to a variety of audiences.”¹¹

Impact of Cybertechnology on Influence Operations

Increasingly, the use of the cyber domain is being actively researched and exploited by the United States and its adversaries to conduct influence operations via cell phone, e-mail, text message, and blogs in both peacetime and combat environments. The cyber world will progressively become both a boon and a bane to IO personnel, allowing a global audience reach but providing a large vulnerability to enemy deception and PSYOP efforts requiring a near immediate response to worldwide operational events.

While traditional forms of MILDEC—operational feints, displays, or instances of camouflage and concealment—are increasingly negated by advancements in intelligence, surveillance, and reconnaissance technology that quickly uncover the deception, cybertechnology has brought a new generation of MILDEC options to military planners.¹² These include digital imagery manipulation, computer file alteration, and false file storage where phony or deceptive electronic files are deliberately made accessible to an adversary.

Ubiquitous Internet availability and the global use of cell phones present new opportunities for PSYOP efforts. The proliferation of cell phone ring tones offers options for embarrassment or message delivery.¹³ For instance, altering a terrorist cell chief or military leader’s ring tone to the refrain “God bless the USA” would cause embarrassment or shame when triggered to ring within earshot of subordinates or superiors. Additionally, some cell phone frequencies are “not detectable to people over the age of 30, while those younger than 30 can hear the frequency,” which enables a targeted audience for some messages.¹⁴ Student revolutionaries in an adversary’s country could be targeted to encourage their antiestablishment activities. In theory, the student could be alerted to a new text message or voice mail with a high-frequency alert tone audible to them without tipping off older, anti-American parents, teachers, or government officials.

The traditional airborne psychological leaflet has been modernized by an Internet version called an “E-flet,” and the loudspeaker is being superseded by text messages delivered to cell phones and called the

“silent loudspeaker.”¹⁵ Messages can even be sent to specific cell phone towers in a given geographic area, thus enabling regular news updates to a target audience to be sent.¹⁶ Again, the student protesters in an adversary’s country could be targeted to receive text messages supporting their activities.

Web sites like *YouTube* and other social networking sites have become a battleground for “a global audience to share firsthand reports, military strategies, propaganda videos, and personal conflict as it unfolds.”¹⁷ This public participation in conflict blurs the lines between combatant and noncombatant when operational data is involved. New counterpropaganda tools aided by the Internet combat this trend.

One method to fight foreign propaganda and lies is for the United States to use a blog or Web site in native languages to educate foreign citizens on political issues and to influence attitudes and advance education on a topic area. For example, if a country holds a constitutional referendum to do away with presidential term limits and the incumbent president is not a US ally, the United States could use the Internet to educate the citizens about the significance and impact of the referendum prior to the vote. Another example is “alert” software, such as “Megaphone,” that notifies a special interest group about chat rooms or Internet polls that are counter to their special interest. This alert enables a counterpropaganda response and offers alternate or contradictory views.¹⁸

The importance of proactively capitalizing on the new range of cyber tools in performing IO missions is surpassed only by the requirement to identify and provide a defense against similar efforts by opponents.

Challenges to Effective Information Operations

While the lanes in the road between MILDEC, PSYOP, and PA seem clear cut in doctrine and theory, cyber operations have blurred the lines between operational missions and authorities due to outdated US laws, Internet technology, global media, and transnational threats. Seven challenges highlight conflicts and uncharted cyber areas in IO that must be addressed if the United States’ national defense is not to be left vulnerable, both legally and defensively. If these areas are not addressed, the United States risks not only the ability to conduct effective cyber-related influence operations but also the capability to effectively employ military instruments of power throughout the range of operations from peacetime to wartime and defend against the same.

Keeping the American Public Informed

The American public plays a large role, both directly and indirectly, in the arena of influence operations. Doctrinally, “MILDEC operations must not intentionally target or mislead the US public, the US Congress, or the US news media.”¹⁹ This insulation of the US public from US deception operations is understandable; however, it also leaves the United States vulnerable to foreign deception and propaganda efforts and “a questioning mind is the first line of defense.”²⁰ Therefore, the general public should be taught how to identify and respond to propaganda, PSYOP, and deception operations launched by any foreign nation or other entity.

In the 2006 war between Israel and Hezbollah, Israel launched an airstrike on 30 July 2006 that allegedly killed as many as 57 civilians. It was later called the Qana massacre in the significant international media coverage.²¹ Ultimately, in light of postbattle assessment, the Qana massacre was determined to actually be “a stage-managed Hezbollah production, designed precisely to enflame international sentiment against Israel and compel the Israelis to accept a ceasefire that would enable the jihad terrorist group to gain some time to recover from the Israeli attacks.”²² The Hezbollah manipulated the attack timeline and doctored photos of recovery workers and corpses to make the air strike appear genocidal and to cover up the military nature of the target. The inconsistencies in the images and the timeline of events were evident upon close scrutiny. Awareness of this type of deception must be developed in the American public and military personnel.

Legal Challenges to Combatant Command Responsibilities

In June 2007, the deputy secretary of defense (DEPSECDEF) issued a “Policy for Department of Defense (DOD) Interactive Internet Activities” memo authorizing the geographic combatant commands to provide information to foreign audiences via two-way communications—e-mail, blogs, chat rooms, and Internet bulletin boards.²³ A “Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences” followed in August 2007, which further authorized geographic COCOMs to produce and maintain “regionally-oriented websites” with “non-interactive” content for foreign audiences.²⁴ By direction, the Web site data must be accurate, truthful, and, in all but cases of operational necessity, attributable. On the surface, it makes sense for a COCOM to use interactive Internet activities (IIA) and regionally focused Web sites to counter extremist activity and thwart proterrorist mind-sets as well as to advance US

political-military interests overseas. However, IIA as defined and structured is the legal responsibility of the DOS and not the DOD.²⁵

The legal crux of the issue is whether these activities are PSYOP, which is a legally defined military mission set, or if they fall into the area of public diplomacy, which is the sole jurisdiction of the DOS.²⁶ While the DEPSECDEF policy letters did direct interagency cooperation with the DOS for international engagement, the term *PSYOP* is never used to define DOD activities. The DOD has limited congressional authority to conduct public diplomacy, and once it “no longer labels its communication measures as PSYOP, it potentially subverts its own statutory authorities to engage foreign audiences.”²⁷ At its core, IIA is public diplomacy conducted as a military mission, yet the appropriation of funds and the use of contractor support for foreign engagement via public diplomacy are more in line with congressional appropriations targeted to the DOS rather than the DOD.²⁸

Modernizing the Smith-Mundt Act

Related to the discussion of geographic COCOM and DOS responsibilities are the legal boundaries in the conduct of US propaganda instituted by the Smith-Mundt Act. Passed in 1948, the US Information and Education Exchange Act, also known as Smith-Mundt, was enacted to counter the worldwide communist propaganda being released by the Soviet Union during the Cold War era. “The Act’s principles are timeless: tell the truth; explain the motives of the United States; bolster morale and extend hope; give a true and convincing picture of American life, methods and ideals; combat misrepresentation and distortion; and aggressively interpret and support American foreign policy.”²⁹ In other words, create a forum for the international release of American news and information (propaganda) to counter the communist propaganda from the Soviet Union, which was “defaming our institutions in the eyes of the peoples of the world.”³⁰

The result was the creation of the US Information Agency (USIA), now a part of DOS, to undertake the mission. Additionally, some well-known media entities are also covered by the Smith-Mundt Act (Voice of America [VOA], Radio Free Asia and Europe, and Radio and TV Marti). A domestic dissemination clause was further strengthened by Congress in 1972 and 1985 to completely “block Americans from accessing USIA materials to the point USIA products were exempt from the Freedom of Information Act.”³¹ In essence, US citizens cannot be trusted to have access to the truthful materials promoting American ideals that are available to the rest of the world.

With the collapse of the Soviet Union and the worldwide communist threat, as well as the shrinking of the world due to the cyber age, a number of Smith-Mundt constraints have outlived their usefulness. First, the Smith-Mundt Act restrictions only cover the current DOS activities previously conducted by USIA, and not those of the entire US government. A 2006 legal review requested by the Defense Policy Analysis Office concluded that “the Act does not apply to the Defense Department.”³² However, based upon implicit congressional support for the act that extends to the government, the DOD has applied the restrictions in its COCOM public outreach activities.³³

The Internet and satellite radio have also made it impossible to separate domestic from international audiences, calling into question whether it is illegal for online products supposedly covered by Smith-Mundt (a DOS or COCOM article produced for foreign consumption) to be accessible by American citizens.

Finally, the ability of the Department of Homeland Security (DHS) and US Northern Command to counter radical ideological products of terrorists, foreign and domestic, requires US truthful information developed by the DOS to be made available. For example, a Minneapolis, Minnesota, community radio station requested permission to re-broadcast a VOA news show that targeted Somalians. The intent was to “offer an informative, Somali-language alternative to the terrorist propaganda that [was] streaming into Minneapolis,” home of the largest Somali community in the United States.³⁴ The VOA, as regulated by the Smith-Mundt Act, denied the request. This example highlights a new strategic vulnerability, the inability to combat a transnational terrorism threat within our own borders.

Countering Adversary Influence Operations

While Smith-Mundt prohibits dissemination of US influence information to American citizens, no corresponding law prohibits foreign nations or organizations from targeting US citizens with propaganda and/or deception. The lack of public awareness of this threat and the proliferation of cheap means for global message distribution leave the US public vulnerable to influence operations (propaganda) and deception by adversaries and other nations. This can include altered imagery, intentional falsehoods, and planted rumors. Some modern examples of influence operations against the US public include the Soviet KGB spreading “bogus stories linking the United States to the creation of HIV/AIDS . . . and [accusing the United States of] employing a Korean civilian airliner as a reconnaissance aircraft over the Kamchatka peninsula. [Additionally], John Kerry appeared in an al-

tered image seated near Jane Fonda at an anti-Vietnam War rally.”³⁵ In order for Americans to recognize another nation’s propaganda, the American educational system should have an information literacy program to ensure that US citizens “have the ability to distinguish truth from falsehood when information is presented.”³⁶

Changing Pejorative Terminology

It seems that the modern usage of the terms *propaganda* and *psychological operations* is generally viewed by Americans as pejorative in nature, in spite of the fact that conventional military IO missions are truthful and accurate. As Hubert H. Humphrey once said, “In real life, unlike in Shakespeare, the sweetness of the rose depends upon the name it bears. Things are not only what they are. They are, in very important respects, what they seem to be.”³⁷

Unfortunately, the words *propaganda* and *psychological operations* have evolved in usage over the past half century to imply deceit and trickery. Thus, the harmful connotation in the minds of Congress, the American public, and even some military leaders impacts negatively on the ability of the US military to effectively conduct influence operations, even truthful ones. When discussions of DOD information operations are made public, the potentially positive effects of the operations are overshadowed by the negative association of the terms themselves. Because the derogatory connotation associated with today’s IO terminology can negatively impact the conduct of the mission and the ability to communicate, a name change should be considered.

Loss of High Ground in the Information Domain

That the United States has no peer competitor in conventional war fighting is not in question. However, the use of nonconventional, asymmetric techniques, particularly those enabled by the Internet, allows nonpeer competitor nation-states and nonnation-state actors a strategic equivalence or an advantage not found in conventional settings. During past conventional conflicts, the US military PA structure could effectively manage the information released to the public by civilian combat newsmen, protecting operations and personnel. However, today’s technology, such as the cell phone, enables everyone the “capability to transmit audio, video and photographs . . . [and] such contributions from the street carry their own form of psychological persuasion.”³⁸ Any incident occurring in a conflict today can be reported, correctly or incorrectly, via Internet chat room, *You-Tube*, cell phone, or text messaging—long before a “legitimate news service can adjudicate its authenticity.”³⁹ A cell phone enables a

group, or even an individual, the ability to conduct unilateral psychological or deception operations against the US, negatively impacting both peacetime and wartime missions by influencing public opinion. This can put pressure on public officials and military leadership regarding conduct, expected outcomes, and even the duration of combat operations.

With the growing dependence on the use of interconnected networks to function in an e-commerce society, cyber weapons are rapidly becoming the “nuclear weapon” of the millennial age. In the past, nuclear weapons were considered the ultimate deterrent and battlefield equalizer, which prompted the creation of international controls on development and possession of such technology. Fortunately, the cost of a nuclear weapons program was prohibitive to all but a handful of sovereign nations. But cybertechnology is inexpensive, easy to obtain, and ubiquitous, thus offering an asymmetric advantage to adversaries, state sponsored and otherwise, to conduct “quite literally, war on the cheap.”⁴⁰ As a result, it is incumbent upon the US military IO community to develop tactics, techniques, and procedures (TTP) for using the new technologies. The military must become proficient in the identification and defeat of foreign attempts at IO and learn to release “precision guided messages . . . to target friendly or enemy soldiers with equal ease.”⁴¹

Defining Neutrality in Cyber Operations

The 1907 Hague Convention requires combatant nations to recognize the rights of neutral nations and that the territory of a neutral nation is inviolable by combatant nations.⁴² The latter neutrality specification causes many questions and is ill defined relative to the realm of cyber operations. The century-old Hague Convention was written when sovereign borders and national boundaries were purely geographic in nature. It must now be reconsidered in the cyber age.

Specifically, the Hague Convention states that, “belligerents may not move forces, weapons, or war materiel across a neutral country’s territory, or conduct hostilities within a neutral’s territory, waters, or airspace. A neutral nation jeopardizes its status if it permits belligerents to engage in such violations.”⁴³ Two primary Internet-based examples highlight the difficulty of applying international laws of neutrality as they pertain to cyber operations—the use of a neutral country’s cyber infrastructure and execution of cyber missions that cross neutral borders.

During the 2006 Israeli-Hezbollah conflict, Israel bombed the Al-Manar facilities in Lebanon prompting Al-Manar (an organization

outlawed in the United States due to its jihadist activities) to rehost its operations on an Austin, Texas-based server owned by Broadwing Communications.⁴⁴ The nature and intent of this rehosting were apparently unknown to Broadwing at the time. It could be argued that Hezbollah is not a sovereign state and the Al-Manar jihadist organization is not a legal combatant, so the Hague and Geneva neutrality conventions were not in play. However, this scenario and similar others demand some very intricate legal discussion on neutrality when cyber conflict occurs between nation-states and nonnation-states, especially the legal and practical consequences of a belligerent “occupying” a neutral nation’s cyber infrastructure.

Another example of Internet rehosting by a belligerent took place in July 2008 in the cyber portion of the conflict between Russia and Georgia. When the Georgian government’s Internet capabilities were rendered virtually nonfunctional by a Russian denial of service attack, Tulip Systems, a US Internet hosting company in Atlanta, “contacted [the] Georgian government officials and offered assistance in reconstituting Georgian Internet capabilities.”⁴⁵ While Tulip Systems provided this assistance without the knowledge or permission of the US government, it calls into question the status of US neutrality during the cyber conflict between these two belligerents. Can a sovereign nation lose its neutral status based upon the unilateral actions of a single citizen?

Another gray area in the realm of cyber neutrality deals with influence operations and the release of E-flets, text messages, or deception efforts (such as altering the contents of a Web site) that involve crossing sovereign borders with respect to physical infrastructure. Similar to the conventions limiting belligerents’ use of radio towers and broadcast equipment in neutral countries, does the execution of a cyber mission traveling across a neutral country’s web infrastructure violate international neutrality laws? The neutrality laws must be modernized or the negative impact to the DOD is obvious.

Recommended Changes to Doctrine and Policy

The breadth of questions raised by the use of cybertechnology in the prosecution of influence operations requires further investigation and correction. To deal with the challenges discussed in the previous section, the following represent some suggested remediation efforts.

As a public service, DHS needs to develop and implement an IO education campaign to develop critical thinking skills to assist the American public in identifying foreign propaganda and deception encountered on the Internet and in cyber media. Additionally, busi-

ness owners of Internet servers would receive education on how their actions in hosting or assisting corporations or nations in countries under cyber attack could put the United States in jeopardy of losing its neutral status and unintentionally becoming a warring party within a conflict.

The DOD must determine whether new legal authorities to undertake Internet-based communications and Web site interactions with foreign audiences are required, as directed by secretary of defense policy letters of 2007. Regardless, the DOD must inform Congress of its public diplomacy (vice PSYOP) efforts and may even need to leave public diplomacy responsibilities to the DOS.⁴⁶

“Congress must undo changes to the Smith-Mundt Act that prevent accountability and effective global engagement. This language, inserted in the 1970’s and 1980’s, prevents transparency and awareness while ignoring the global movement of information and people.”⁴⁷ Congress must amend Smith-Mundt to remove the ban on domestic dissemination of materials originally developed for foreign audiences. “In this age of communication without borders, the existence of such statutory language only subverts America’s most powerful tool of soft power: our ideals.”⁴⁸

Change the terms *propaganda* and *PSYOP* to something less pejorative to the American public. Hubert H. Humphrey once stated, “Propaganda, to be effective, must be believed. To be believed, it must be credible. To be credible, it must be true.”⁴⁹ Given that IO and PA activities in conventional military operations are factual and truthful, the pejorative terms in use hinder the accomplishment of the mission. New terminology could be as simple as *operational communications*, *strategic effects*, *broadcast operations*, or *CYOP* (cyber psychological operations).⁵⁰

Update US influence operations doctrine to include cybertechnology. Specifically, develop TTPs for employing PSYOP, MILDEC, and PA using the new cybertechnology. Once developed, the TTPs must be incorporated into all applicable military exercises to allow the military IO operator an avenue for developing proficiency in the release of “precision-guided messages” to foreign audiences.⁵¹

Codify a US cyber policy on cyber neutrality that includes belligerent and neutral nation responsibilities. Since international law is often derived from common practice, the United States can be in the forefront of shaping international cyber neutrality laws and sovereign nation responsibilities when a “belligerent takes cyber refuge in a neutral country’s territory.”⁵² Ultimately, this requires a worldwide collaborative effort to “create a single set of cyber laws and procedures internationally in order to insure that there is no safe harbor

for cyber criminals.”⁵³ Cyber criminals would include state and non-state actors threatening our security.

Putting It All Together—Operational Examples

Assuming all of the previous challenges are addressed and resolved, the following example summarizes how the military commander can benefit from information operations in the cyber age. The examples use radical Islamic extremists as the notional enemy.

As radical Islam extremists expertly use the Internet and global media to publicize and advance their propaganda and lies, an educated American civilian and military population can recognize misinformation and deception using critical thinking skills, asking hard questions, and seeking alternate or corroborating sources of information before making judgments or believing the foreign stories. With a Smith-Mundt Act modification, DHS, in conjunction with the Northern Command, can provide a direct counterinformation campaign within US borders via the Internet, radio, and television (in English and other foreign languages). This campaign will reduce the domestic threat from misinformed potential terrorist recruits living in the United States.

Once cyber TTPs are codified and a well trained cadre of military professionals developed, the combatant commander will be able to informationally bombard Islamic terrorists and their potential supporters by sending precision-guided messages to specific cell towers, cell phones, e-mail, or Web sites as part of a public diplomacy or CYOP effort.⁵⁴ The ability to incorporate these tools as standard procedures will enhance a counterinsurgency campaign by actively persuading less radical terrorists and sympathizers to give up the fight without resorting to expensive (both monetarily and socially) conventional warfare.

Once international norms are established for cyber-based laws of armed conflict, commanders will better understand legal boundaries to recognizing, initiating, and defending against cyber warfare. This, in turn, leaves a training and education task for both the military professionals and the American information technology public. But, until those norms are codified, the United States is at risk of unintentionally becoming a belligerent in other countries' conflicts, having our military and civilian cyber professionals unwittingly held liable under the international court of justice or not recognizing that a cyber war attack has taken place against our nation, thus forfeiting our opportunity for a prompt and appropriate response.

Conclusion

The remediation actions and operational examples outlined in this thesis are not exhaustive and still leave a large gray area in the realm of influence operations and the use of cybertechnology. They do represent a start, however, in identifying doctrinal gaps, outdated legal roadblocks, and deficiencies in policies, laws, and education. The United States must “amend existing policies to allow [influence operations] to embrace the range of contemporary media . . . as an integral asset” to military operations.⁵⁵ These changes would provide structure to largely disorganized and unnecessarily constrained efforts to fully employ cybertechnology and provide a new opportunity for the United States to conduct effective and efficient influence operations using that technology. Without addressing these challenges promptly, the national security of our nation is at risk in current and future conflicts.

Notes

1. JP 3-13, *Information Operations*, 13 February 2006, I-1.
2. *Ibid.*, II-8-9.
3. JP 3-13.4, *Military Deception*, 13 July 2006, vii. *Perfidy* is “the use of unlawful or prohibited deceptions. Acts of perfidy are deceptions designed to invite the confidence of the enemy leading to the belief that he/she is entitled to, or is obliged to accord, protected status under the law of armed conflict, with the intent to betray that confidence. Acts of perfidy include but are not limited to: feigning surrender or waving a white flag to lure the enemy into a trap; misusing protective signs, signals, and symbols to injure, kill, or capture the enemy; using an ambulance or medical aircraft marked with the red cross or red crescent to carry armed combatants, weapons, or ammunition in order to attack or elude enemy forces; and using false, deceptive, or neutral flags, insignia, or uniforms [in actual combat].” *Ibid.*, I-8.
4. Sun Tzu, *The Art of War*, ed. and trans. Samuel Griffith (London: Oxford University Press, 1963), 66.
5. JP 3-13.4, *Military Deception*, I-7. A *ruse* is “a cunning trick designed to deceive the adversary to obtain friendly advantage. It is characterized by deliberately exposing false or confusing information for collection and interpretation by the adversary.” *Ibid.*, I-7.
6. Daniel Silverberg and Joseph Heimann, “An Ever-Expanding War: Legal Aspects of Online Strategic Communication,” *Parameters*, Summer 2009, 80.
7. JP 3-13.2, *Psychological Operations*, 7 January 2010, vii.
8. *Wikipedia*, s.v. “Propaganda,” <http://en.wikipedia.org/wiki/Propaganda> (accessed 25 January 2010).
9. JP 3-61, *Public Affairs*, 9 May 2006, xi.
10. *Ibid.*, II-1
11. Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, 11 January 2005, 5.
12. JP 3-13.4, *Military Deception*, I-7. A *feint* is “an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary of the location and/or time of the actual main offensive action.” *Displays* are “the simulation,

disguising, and/or portrayal of friendly objects, units, or capabilities in the projection of the military deception story. Such capabilities may not exist but are made to appear so (simulations)." *Ibid.*, 1-7.

13. Timothy L. Thomas, "Hezbollah, Israel, and Cyber Psyop," *IO Sphere*, Winter 2007, 31.

14. *Ibid.*

15. *Ibid.*

16. *Ibid.*, 32.

17. *Ibid.*

18. *Ibid.*

19. JP 3-13.4, *Military Deception*, II-8

20. Scot Macdonald, *Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations* (New York: Routledge, 2007), 178.

21. Robert Spencer, "Stage-Managed Massacre," *Frontpagemag.com*, 2 August 2006, <http://97.74.65.51/readArticle.aspx?ARTID=3281> (accessed 13 February 2010).

22. *Ibid.*

23. Gordon England, deputy secretary of defense, "Policy for Department of Defense (DOD) Interactive Internet Activities," policy memorandum, 8 June 2007.

24. Gordon England, deputy secretary of defense, "Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences," policy memorandum, 3 August 2007.

25. Silverberg and Heimann, "Ever-Expanding War."

26. *Ibid.*, 78

27. *Ibid.*

28. *Ibid.*

29. Matt Armstrong, "Smith-Mundt Act," *Small Wars Journal*, 28 July 2008.

30. *Ibid.*

31. *Ibid.*

32. *Ibid.*

33. *Ibid.*

34. Matt Armstrong, "Censoring the Voice of America," *Foreign Policy*, 6 August 2009.

35. Macdonald, *Propaganda and Information Warfare*, 182.

36. *Ibid.*

37. Hubert H. Humphrey, *Quoteopia.com*, <http://www.quoteopia.com/famous.php?quotesby=huberthumphrey> (accessed 13 February 2010).

38. Thomas, "Hezbollah, Israel, and Cyber Psyop," 30.

39. *Ibid.*

40. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, research publication (Colorado Springs, CO: Institute for Information Technology Applications, 1999), 10.

41. Thomas, "Hezbollah, Israel, and Cyber Psyop," 30.

42. Stephen W. Kornis and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Winter 2008-9, 62.

43. *Ibid.*

44. Thomas, "Hezbollah, Israel, and Cyber Psyop," 33.

45. Kornis and Kastenberg, "Georgia's Cyber Left Hook," 67.

46. Silverberg and Heimann, "Ever-Expanding War," 90.

47. Armstrong, "Smith-Mundt Act."

48. Gregory L. Garland, "Editorials and Op-Eds," *AmericanDiplomacy.Org*, 3 January 2009, www.unc.edu/depts/diplomat/item/2009/0103/ed/garland_smithmundt.html (accessed 23 October 2009).

49. Hubert H. Humphrey, *BrainyQuote.com*, http://www.brainyquote.com/quotes/authors/h/hubert_h_humphrey_2.html (accessed 13 February 2010).
50. Thomas, "Hezbollah, Israel, and Cyber Psyop"; and AFDD 2-5: *Information Operations*, 30.
51. Thomas, "Hezbollah, Israel, and Cyber Psyop."
52. Korn and Kastenberg, "Georgia's Cyber Left Hook," 66.
53. Paul Rosenzweig, "National Security Threats in Cyberspace," McCormick Foundation Conference series (Wheaton, IL: McCormick Foundation, 2009), 30.
54. Thomas, "Hezbollah, Israel, and Cyber Psyop."
55. Angela Maria Lungu, "War.com: The Internet and Psychological Operations," *Joint Forces Quarterly*, Spring/Summer 2001, 13–17.

Abbreviations

AFDD	Air Force doctrine document
COCOM	combatant command
CYOP	cyber psychological operations
DEPSECDEF	deputy secretary of defense
DHS	Department of Homeland Security
DOD	Department of Defense
DOS	Department of State
E-flet	Internet psychological leaflet
IIA	interactive Internet activities
IO	information operations
JP	joint publication
MILDEC	military deception
PA	Public Affairs
PSYOP	psychological operations
TTP	tactics, techniques, and procedures
USIA	US Information Agency
VOA	Voice of America