AIR WAR COLLEGE

AIR UNIVERSITY

INFLUENCE OPERATIONS AND THE INTERNET: A 21ST CENTURY ISSUE

by

Rebecca A. Keller, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

17 February 2010

[Cleared for public release 7/2/2010; AETC-2010-0439]

DISCLAIMER

BIOGRAPHY

Lt Col Rebecca A. Keller received her Air Force commission in 1988 through ROTC at the University of St Thomas, in St Paul, Minnesota. She is a career intelligence officer that also had one career broadening tour in the computer and communications career field. Her intelligence assignments have been varied and include many intelligence disciplines (SIGINT, IMINT, Targeting, Information Operations, and Collection Management). She has held positions of flight commander, operations officer, squadron commander, and deputy division chief on a MAJCOM staff.

INTRODUCTION

The conduct of information operations (IO), which includes military deception (MILDEC) and psychological operations (PSYOP), by the United States military, is based on both doctrinal precedence and operational necessity. The increasing use of cyber technology 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 first defines relevant terminology and then identifies current operational and legal constraints in the execution of IO using cyber technology. 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 (IO)

According to *Joint Publication 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 psychological operations (PSYOP) and military deception (MILDEC), while Public Affairs (PA) is considered an *Information Operations related capability*.[2] All three of these activities are inherent in the conduct of military operations from peace to war and are increasingly affected by cyber technology. In order to understand these missions, it is important to first explain their definitions and functions.

---

[1] United States. *Joint Publication 3-13: Information Operations.* Washington DC: Department of Defense, 2006. I-1
[2] Ibid., II-8-9

Military Deception (MILDEC) Involvement in IO

Short of perfidy[3], the intent of MILDEC, according *Joint Publication 3-13.4: Military Deception* is the execution of actions "to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations."[4] Deception has been a recognized component of war for millennia; nearly 2,500 years ago Chinese military strategist Sun Tzu stated "all warfare is based on deception."[5] In modern times, two classic examples of military deception are 1.) Operation MINCEMEAT, the World War II deception strategy which convinced the Germans that the Allies were preparing to invade Greece instead of Italy, and 2.) A perfectly executed ruse[6] by the Egyptians and Syrians when they made it appear they were holding a military exercise and instead initiated the 1973 Arab-Israeli War catching the Israelis completely off guard.

Psychological Operations (PSYOP) Involvement in IO

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.[7] *Joint Publication 3-13.2, Psychological Operations,* says the purpose of PSYOP is to influence foreign audience perceptions and behavior as part of approved programs

---

[3] Per JP3-13.4, the use of unlawful or prohibited deceptions is called "perfidy." Acts of perfidy are deceptions designed to invite the confidence of the enemy to lead him to believe that he 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 in order to lure the enemy into a trap; misuse of protective signs, signals, and symbols in order 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 the use in actual combat of false, deceptive, or neutral flags, insignia, or uniforms.
[4] United States. *Joint Publication 3-13.4: Military Deception.* Washington DC: Department of Defense. vii
[5] Griffith, Samuel (translator). *Sun Tzu: The Art of War*. London: Oxford University Press, 1963. 66.
[6] Per JP3-13.4, 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.
[7] Silverberg, Daniel and Heimann, Joseph. "An Ever-Expanding War: Legal Aspects of Online Strategic Communication." Parameter, Summer, 2009: 80.

supporting US policy and military objectives.[8] Since World War I, the United States has conducted airborne delivery of 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 whereby military ground personnel, aircraft, or ships are a visible reminder to foreign nations of US combat capabilities.

Propaganda Involvement in IO

Propaganda is "a form of communication aimed at influencing the attitude of a community toward some cause or position."[9] While historically not a pejorative term, today the terms PSYOP and propaganda are often freely interchanged and both have taken primarily derogatory connotations in spite of the fact that both provide important national security tools and are truthful in content during the execution of conventional military operations.

Public Affairs (PA) Involvement in IO

Where PSYOP and propaganda are communications directed at foreign audiences, military Public Affairs (PA) offices provide to journalists and the American public similar information, to articulate DoD positions on policies and operations. The activities of Public Affairs professionals are guided by the same principles as civilian journalists and are based upon the freedom of the press. Military PA responsibilities are captured in *Joint Publication 3-61, Public Affairs*, and include "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

[8] United States. *Joint Publication 3-13.2: Psychological Operations*. Washington DC: Department of Defense. vii
[9] Wikipedia Online Encyclopedia. *Entry for Propaganda.* http://en.wikipedia.org/wiki/Propaganda (accessed January 25, 2010).

friends and allies."[10] Even President Abraham Lincoln understood the importance of interacting with the public when he stated, "public opinion is everything. With it, nothing can fail. Without it, nothing can succeed."[11]

Department of State (DoS) Involvement in IO

The requirement to influence foreign attitudes and behaviors is not unique to DoD, and in fact, the responsibility of the Department of State's public diplomacy efforts can often overlap with military PSYOP or PA activities. Out of necessity, State Department public diplomacy and military PA attempt to 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."[12]

Impact of Cyber Technology on Influence Operations

Increasingly, the use of the cyber domain is being actively researched and exploited by the United States and our adversaries to conduct influence operations via cell phones, email, text messages, and blogs in both peacetime and combat environments. The cyber world will progressively become both a boon and a bane to IO personnel, allowing them to reach a global audience, but also providing a large vulnerability to enemy deception and PSYOP efforts that will require a near immediate response to worldwide, operational events.

New Cyber Opportunities for MILDEC

While traditional forms of MILDEC in the guise of operational feints[13], displays[14] or instances of camouflage and concealment are increasingly negated by advancements in

---

[10] United States. *Joint Publication 3-61: Public Affairs*. Washington DC: Department of Defense. xi
[11] Ibid, II-1
[12] United States. *Air Force Doctrine Document 2-5: Information Operations*. Washington DC: Department of Defense. 5
[13] Per JP 3-13.4, a feint is an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary as to the location and/or time of the actual main offensive action.

intelligence, surveillance, and reconnaissance technology that quickly uncover the deception, cyber technology has brought a new generation of MILDEC options to military planners. These include digital imagery manipulation, computer file alteration, and false file storage where phony or deceptive electronic files are deliberately made accessible for an adversary.

New Cyber Opportunities for PSYOP

Ubiquitous internet availability, and the global use of cell phones, presents new opportunities for our PSYOP efforts. The proliferation of cell phone ring tones offers options for embarrassment or message delivery.[15] For instance, we could alter the cell phone of a terrorist cell chief or military leader so that the refrain "God bless the USA" became the ring tone, enabling us to cause embarrassment or shame by triggering the phone to ring within earshot of subordinates or superiors. Additionally, there are some cell phone frequencies that are normally "not detectable to people over the age of 30, while those younger than 30 can hear the frequency,"[16] which enables a targeted audience for some messages. For example, we could target student revolutionaries in an adversary country to encourage their anti-establishment 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 also been modernized by an internet version called an "E-flet,"[17] and the loudspeaker is being superseded by text messages delivered to cell phones and called the "silent loudspeaker." We can even send messages to specific cell

---

[14] Displays are the simulation, disguising, and/or portrayal of friendly objects, units, or capabilities in the projection of the MILDEC story. Such capabilities may not exist, but are made to appear so (simulations).
[15] Thomas, Timothy L. "Hezballah, Israel, and Cyber Psyop." IO Sphere, Winter 2007: 31
[16] Ibid
[17] Thomas, Timothy L. "Hezballah, Israel, and Cyber Psyop." IO Sphere, Winter 2007: 31

phone towers in a given geographic area, thus enabling us to send regular news updates to a target audience.[18] Again, the student protestors in an adversary country could be a targeted audience to receive texts of support for their activities.

New Opportunities for Social Networking

Websites 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."[19] This public participation in conflict begins to blur the lines between combatant and non-combatant when operational data is involved. To combat this trend there are new counterpropaganda tools aided by the internet.

One method for combating foreign propaganda and lies is for the US to use a blog or website in native languages to educate foreign citizens on political issues, in order to influence attitudes and advance education on a topic area. For instance, if a country were holding a constitutional referendum to do away with presidential term limits and the incumbent president was not an ally of the US, we 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, enabling them to respond with their own counterpropaganda and offer alternate or contradictory views.[20]

The importance for the United States to proactively capitalize 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.

---

[18] Ibid, 32.
[19] Ibid.
[20] Thomas, Timothy L. "Hezballah, Israel, and Cyber Psyop." IO Sphere, Winter 2007: 32.

Challenges to Effective IO

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. The seven information operations challenges below highlight conflicts and uncharted cyber areas in information operations that must be addressed if our national defense is not to be left vulnerable, both legally and defensively. Without addressing these areas the United States puts at risk not only our ability to conduct effective cyber-related influence operations, but also our ability to effectively employ our military instrument of power throughout the range of operations from peacetime to war 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."[21] This insulation of the US public from US deception operations is understandable; however, it also leaves the US vulnerable to foreign deception and propaganda efforts and "a questioning mind is the first line of defense."[22] Therefore, we are failing our military leadership and the general public if we do not teach them 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 Hizbollah, Israel launched an airstrike on 30 July 2006, that allegedly killed as many as 57 civilians and was later called the Qana Massacre in the

---

[21] United States. *Joint Publication 3-13.4: Military Deception*. Washington DC: Department of Defense. II-8
[22] Macdonald, Scot. *Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations* . New York: Routledge, 2007: 178.

significant international media coverage it received.[23] Ultimately, in the light of post-battle assessment, it was determined the Qana Massacre was actually "a stage-managed Hizballah 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."[24] The Hizballah had manipulated the timeline of the attack, and doctored photos of recovery workers and corpses, both to make the air strike appear genocidal and to cover up the military nature of the target. The inconsistencies in both the images and the timeline of events were evident upon close scrutiny. It is awareness of this type of deception that must be developed in the American public and military personnel.

Legal Challenges to Combatant Command (COCOM) Responsibilities

In June 2007, the Deputy Secretary for Defense (DEPSECDEF) issued a "Policy for Department of Defense (DoD) Interactive Internet Activities," authorizing the geographic Combatant Commands to provide information to foreign audiences via two-way communications—like email, blogs, chat rooms, and internet bulletin boards.[25] This memo was followed in August of the same year with a "Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences," which further authorized geographic COCOMs to produce and maintain "regionally-oriented websites" with "non-interactive" content for foreign audiences.[26] By direction, the website data must be accurate and truthful, and in all but cases of operational necessity, it must be attributable. On the surface, it makes sense for a COCOM to use Interactive Internet Activities (IIA) and regionally focused websites to counter

[23] Spencer, Robert. "Stage-Managed Massacre." *Frontpagemag.com.* Aug 02, 2006. http://97.74.65.51/readArticle.aspx?ARTID=3281 (accessed Feb 13, 2010)
[24] Ibid
[25] Deputy Secretary of Defense. "Policy for Department of Defense (DoD) Interactive Internet Activities." Official Memorandum. Washington DC: Pentagon, June 8, 2007.
[26] Deputy Secretary of Defense. "Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences." Official Memorandum. Washington DC: Pentagon, August 3, 2007.

extremist activity and thwart pro-terrorist mindsets, as well as advance US political-military interests overseas. However, IIA as defined and structured above is the legal responsibility of the Department of State (DoS) and not the Department of Defense.[27]

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.[28] While the DEPSECDEF policy letters did direct interagency cooperation with the DoS for international engagement, they never used the term PSYOP to define the 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."[29] At its core, IIA is public diplomacy being 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 State Department, rather than to DoD.[30]

Modernizing the Smith-Mundt Act

Related to the previous discussion of geographic COCOM and DoS responsibilities, are the legal boundaries instituted by the Smith-Mundt Act in the conduct of US propaganda. First 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

---

[27] Silverberg, Daniel and Heimann, Joseph. "An Ever-Expanding War: Legal Aspects of Online Strategic Communication." Parameter, Summer, 2009.
[28] Ibid., 78
[29] Ibid
[30] Silverberg, Daniel and Heimann, Joseph. "An Ever-Expanding War: Legal Aspects of Online Strategic Communication." Parameter, Summer, 2009.

of American life, methods and ideals; combat misrepresentation and distortion; and aggressively interpret and support American foreign policy."[31] In other words, create a forum for the international release of American news and information (aka. propaganda) to counter the communist propaganda from the USSR which was "defaming our institutions in the eyes of the peoples of the world."[32]

The result was the creation of the US Information Agency (USIA), now a part of the State Department, to undertake this mission. Additionally, some well known media entities are also covered by the Smith-Mundt Act (for example, Voice of America (VOA), Radio Free Asia and Europe, and Radio and TV Marti). The act contained a domestic dissemination clause that was further strengthened by Congress in 1972 and 1985 in order to completely "block Americans from accessing USIA materials to the point USIA products were exempt from the Freedom of Information Act."[33] 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 worldwide communist threat, as well as the shrinking of the world due to the cyber age, there are a number of Smith-Mundt constraints that have outlived their usefulness. First, the Smith-Mundt Act restrictions only cover the current Department of State activities that were previously conducted by USIA, and not those of the entire US Government. A 2006 legal review requested by the Defense Policy Analysis Office "concluded the Act does not apply to the Defense Department."[34] However, based upon implicit

---

[31] Armstrong, Matt. "The Smith-Mundt Act: Myths, Facts and Recommendations." MountainRunner. November 24, 2009. http://mountainrunner.us/files/s-m/rethinking_smith_mundt.pdf (accessed December 7, 2009).
[32] Ibid
[33] Ibid
[34] Armstrong, Matt. "The Smith-Mundt Act: Myths, Facts and Recommendations." MountainRunner. November 24, 2009. http://mountainrunner.us/files/s-m/rethinking_smith_mundt.pdf (accessed December 7, 2009).

Congressional support for the Smith-Mundt Act that extends to the entirety of the Government, the Defense Department has applied the restrictions in its COCOM public outreach activities.[35]

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

Finally, the ability of the Department of Homeland Security and US Northern Command to counter radical ideological products of terrorists, foreign and domestic, requires the ability to make available within the US truthful information developed by the DoS. For example, a community radio station in Minneapolis, Minnesota, requested permission to rebroadcast a news show from Voice of America that targeted Somalians. The intent was to "offer an informative, Somali-language alternative to the terrorist propaganda that [was] streaming into Minneapolis,"[36] home of the largest Somali community in the US. The VOA, as regulated by the Smith-Mundt Act, denied the request for Somali language radio programming. This example highlights a new strategic vulnerability, our 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 our own citizens, there is no corresponding law that prohibits foreign nations or organizations from targeting US citizens with their 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 (aka propaganda) and deception by adversaries and

[35] Ibid
[36] Armstrong, Matt. "Censoring the Voice of America." *Foreign Policy*, August 6, 2009: 1.

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 US of] employing a Korean civilian airliner as a reconnaissance aircraft over the Kamchatka peninsula. [Additionally], John Kerry appeared in an altered image seated near Jane Fonda at an anti-Vietnam War rally."[37] In order for Americans to recognize another nation's propaganda, our educational system should have an information literacy program to ensure US citizens "have the ability to distinguish truth from falsehood when information is presented."[38]

Changing Pejorative Terminology

It seems the modern usage of the terms *propaganda* and *psychological operations* are 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."[39] Unfortunately, the IO words above have evolved in usage over the past half century to imply deceit and trickery. Thus, the negative connotation of the above terms 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.

---

[37] Macdonald, Scot. Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations. New York: Routledge, 2007. 182.
[38] Ibid
[39] Humphrey, Hubert H. *Quoteopia.* http://www.quoteopia.com/famous.php?quotesby=huberthhumphrey (accessed Feb 13, 2010).

Because the derogatory connotation associated with today's IO terminology can negatively impact the conduct of the mission and our ability to communicate, a name change should be considered.

Loss of Highground in the Information Domain

That the United States has no peer competitor in conventional warfighting is not in question. However, the use of non-conventional, asymmetric techniques, particularly those enabled by the internet, allows non-peer competitor nation states and non-nation state actors a strategic equivalence or even advantage not found in a conventional setting. During past conventional conflicts the US military public affairs 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."[40] Any incident occurring in a conflict today can be reported, correctly or incorrectly, via internet chat room, YouTube, cell phone, or text messaging—long before a "legitimate news service can adjudicate its authenticity."[41] A simple cell phone enables a group, or even an individual, the ability to conduct unilateral psychological or deception operations against the US, operations that can negatively impact both peacetime and wartime missions by influencing public opinion, which in turn can put pressure on public officials and military leadership regarding conduct, expected outcomes, and even the duration of combat operations.

With the growing dependence by Soviets and the military on the use of interconnected networks to function in an e-commerce society, cyber weapons are rapidly becoming the

[40] Thomas, Timothy L. "Hezballah, Israel, and Cyber Psyop." IO Sphere, Winter 2007: 30.
[41] Thomas, Timothy L. "Hezballah, Israel, and Cyber Psyop." IO Sphere, Winter 2007: 30.

"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 cyber technology is inexpensive, easy to obtain, and ubiquitous, thus offering an asymmetric advantage to our adversaries, state-sponsored and otherwise, to conduct "quite literally, war on the cheap."[42] As a result, it is incumbent upon the US military IO community to develop tactics, techniques, and procedures (TTP) for using the new technologies. We also must become proficient in the identification and defeat of foreign attempts at information operations, and learn to release our own "precision guided messages…to target friendly or enemy soldiers with equal ease."[43]

Defining Neutrality in Cyber Operations

The 1907 Hague Convention requires combatant nations to recognize the rights of neutral nations and further states that the territory of a neutral nation is inviolable by the combatant nations.[44] 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, "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

[42] Schmitt, Michael N. Computer Network Attack and the use of Force in International Law: Thoughts on a Normative Framework. Research Publication, Colorado Springs: Institute for Information Technology Applications, 1999: 10
[43] Thomas, Timothy L. "Hezballah, Israel, and Cyber Psyop." IO Sphere, Winter 2007: 30.
[44] Korns, Stephen W. and Kastenberg, Joshua E. "Georgia's Cyber Left Hook." Parameters, Winter 2008-2009: 62

engage in such violations."[45] Two primary internet-based examples highlight the difficulty of applying international laws of neutrality as they pertain to cyber operations. The first is the use of a neutral country's cyber infrastructure and the second is the execution of cyber missions that cross neutral borders.

During the 2006 Israeli-Hizballah conflict, Israel bombed the Al-Manar facilities in Lebanon prompting Al-Manar (an organization outlawed in the US, due to its jihadist activities) to re-host its operations on a server owned by Broadwing Communications in Austin, Texas.[46] The nature and intent of this rehosting was apparently unknown to Broadwing at the time. One could argue that the Hizballah is not a sovereign state and the Al-Manar jihadist organization is not a legal combatant, and therefore, Hague and Geneva neutrality conventions were not in play. However, this scenario and others like it demand some very intricate legal discussion on neutrality when cyber conflict occurs between nation states and non-nation 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 non-functional 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."[47] While Tulip Systems provided this assistance without the knowledge or permission of the United States government, it calls into question the status of US neutrality during the cyber conflict between

---

[45] Korns, Stephen W. and Kastenberg, Joshua E. "Georgia's Cyber Left Hook." Parameters, Winter 2008-2009: 62
[46] Thomas, Timothy L. "Hezballah, Israel, and Cyber Psyop." IO Sphere, Winter 2007: 33
[47] Korns, Stephen W. and Kastenberg, Joshua E. "Georgia's Cyber Left Hook." Parameters, Winter 2008-2009: 67

these two belligerents. Can a sovereign nation lose its neutral status based upon the unilateral actions of a single citizen?

Another grey area in the realm of cyber neutrality deals with influence operations and the release of E-flets, text messages or even deception efforts, like altering the contents of a website, 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 that happens to travel across a neutral country's web infrastructure violate international neutrality laws? The neutrality laws must be modernized or the negative impact to DoD is obvious.

Recommended Changes to Doctrine and Policy

The breadth of questions raised by the use of cyber technology 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:

Implement a US Education Campaign

As a public service, a federal agency, for instance the Department of Homeland Security, needs to develop and implement an information operations education campaign for the American public. The intent would be to develop critical thinking skills to assist the public in identifying foreign propaganda and deception encountered on the internet and in cyber media. Additionally, business owners of internet servers would be educated on how their actions in hosting or assisting corporations or nations in countries under cyber attack could put the US in jeopardy of losing its neutral status and unintentionally becoming a warring party within a conflict.

Examine DoD Legal Authorities for Public Diplomacy Missions

DoD must determine whether it requires new legal authorities to undertake internet-based communications and web-site interactions with foreign audiences, as directed by SECDEF policy letters of 2007. Regardless, DoD must inform Congress of its public diplomacy (vice PSYOP) efforts. DoD may even need to leave public diplomacy responsibilities to the DoS.[48]

Revise the Smith-Mundt Act

"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."[49] 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."[50]

Develop Less Pejorative IO Terminology

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."[51] Given that Information Operations and Public Affairs activities in conventional military operations are factual and truthful, the pejorative terms in use hinder the accomplishment of the mission. New terminology

---

[48] Silverberg, Daniel and Heimann, Joseph. "An Ever-Expanding War: Legal Aspects of Online Strategic Communication." Parameter, Summer, 2009: 90

[49] Armstrong, Matt. "The Smith-Mundt Act: Myths, Facts and Recommendations." MountainRunner. November 24, 2009. http://mountainrunner.us/files/s-m/rethinking_smith_mundt.pdf (accessed December 7, 2009)

[50] Garland, Gregory L. "Editorials and Op-Eds." *AmericanDiplomacy.Org.* Jan 3, 2009 www.unc.edu/depts/diplomat/item/2009/0103/ed/garland_smithmundt.html (accessed Oct 23, 2009)

[51] Humphrey, Hubert H. *Brainy Quote.* http://www.brainyquote.com/quotes/authors/h/hubert_h_humphrey_2.html (accessed Feb 13, 2010)

could be as simple as *operational communications*, *strategic effects*, *broadcast operations*, or even *CYOP*, which stands for "cyber psychological operations."[52]

Include Cyber Technology in Existing Doctrine

Update US Influence Operations doctrine to include cyber technology. Specifically, develop TTPs for employing PSYOP, MILDEC, and Public Affairs using the new cyber technology. 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"[53] to foreign audiences.

Develop a Policy on Cyber Neutrality

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 US can be in the forefront of shaping international cyber neutrality laws and responsibilities of sovereign nations when a "belligerent takes cyber refuge in a neutral country's territory."[54] Ultimately, this requires a worldwide collaborative effort to "create a single set of cyberlaws and procedures internationally in order to insure that there is no safe harbor for cyber criminals."[55] 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 notional example summarizes the ease of which the military commander can benefit from

---

[52] Thomas, Timothy L. "Hezballah, Israel, and Cyber Psyop." *IO Sphere*, Winter 2007: 30-35
United States Air Force. *Air Force Doctrine Document 2-5: Information Operations.* Washington DC: Department of Defense, 2005, 30
[53] Thomas, Timothy L. "Hezballah, Israel, and Cyber Psyop." IO Sphere, Winter 2007
[54] Korns, Stephen W. and Kastenberg, Joshua E. "Georgia's Cyber Left Hook." Parameters, Winter 2008-2009: 66
[55] Rosenzweig, Paul. "National Security Threats in Cyberspace." McCormick Foundation ConferenceSeries. Wheaton: McCormick Foundation, 2009. 30

information operations in the cyber age. The examples use radical Islamic extremists as the notional enemy.

As radical Islam extremists expertly use both the internet and global media to publicize and advance their propaganda and lies, an educated American civilian and military population will recognize instances of 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. Likewise, given a modification of the Smith-Mundt Act, the Department of Homeland Security in conjunction with NORTHCOM, will be able to provide a direct counter-information campaign via the internet, radio and television (in both English and other foreign languages) within US borders, to reduce the domestic threat from misinformed potential terrorist recruits living in our country.

Once cyber TTPs are codified and a well trained cadre of military professionals is developed, the combatant commander will be able to informationally bombard Islamic terrorists and their potential supporters by sending "precision guided messages"[56] to specific cell towers, cell phones, emails or internet websites, as part of a public diplomacy or CYOP effort. The ability to incorporate these tools as standard procedures will enhance a counter-insurgency 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 IT public. But, until those norms are codified, the US is at risk

[56] Thomas, Timothy L. "Hezballah, Israel, and Cyber Psyop." IO Sphere, Winter 2007

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 perhaps even worse, not recognizing that a cyberwar 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 grey area in the realm of influence operations and the use of cyber technology. They do represent a start, however, in identifying doctrinal gaps, outdated legal roadblocks and deficiencies in policies, laws, and education. We must "amend existing policies to allow [influence operations] to embrace the range of contemporary media…as an integral asset" to military operations.[57] These changes would begin to provide structure to largely disorganized and unnecessarily constrained efforts to fully employ cyber technology and provide a new opportunity for the United States to conduct effective and efficient influence operations using that technology. Without addressing these challenges promptly we put the national security of our nation at risk in current and future conflicts.

[57] Lungu, Angela Maria. "War.com: The internet and Psychological Operations." Joint Forces Quarterly, Spring/Summer 2001: 17

Bibliography

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

—. "Rethinking Smith-Mundt." Small Wars Journal, 2008.

—. "The Smith-Mundt Act: Myths, Facts and Recommendations." MountainRunner. November 24, 2009. http://mountainrunner.us/files/s-m/rethinking_smith_mundt.pdf (accessed December 7, 2009).

Deputy Secretary of Defense. "Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences." Official Memorandum. Washington DC: Pentagon, August 3, 2007.

—. "Policy for Department of Defense (DoD) Interactive Internet Activities." Official Memorandum. Washington DC: Pentagon, June 8, 2007.

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

Griffith, Samuel (Translator). Sun Tzu: The Art of War. London: Oxford University Press, 1963.

Humphrey, Hubert H. Quoteopia. http://www.quoteopia.com/famous.php?quotesby=huberthhumphrey (accessed Feb 13, 2010).

Kilcullen, David. The Accidental Guerrilla. New York: Oxford Press, 2009.

Korns, Stephen W. and Kastenberg, Joshua E. "Georgia's Cyber Left Hook." Parameters, Winter 2008-2009: 60-76.

Lungu, Angela Maria. "War.com: The internet and Psychological Operations." Joint Forces Quarterly, Spring/Summer 2001: 13-17.

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

Pumphrey, Carolyn and Antulio Echevarria. "Strategic Deception in Modern Democracies: Ethical, Legal, and Policy Challenges." Strategic Studies Institute. Carlisle: US Army War College, 2003. 4.

Rosenzweig, Paul. "National Security Threats in Cyberspace." McCormick Foundation Conference Series. Wheaton: McCormick Foundation, 2009. 30.

Schmitt, Michael N. Computer Network Attack and the use of Force in International Law: Thoughts on a Normative Framework. Research Publication, Colorado Springs: Institute for Information Technology Applications, 1999.

Silverberg, Daniel and Heimann, Joseph. "An Ever-Expanding War: Legal Aspects of Online Strategic Communication." Parameter, Summer, 2009: 77-93.

Spencer, Robert. "Stage-Managed Massacre." Frontpagemag.com. Aug 02, 2006. http://97.74.65.51/readArticle.aspx?ARTID=3281 (accessed Feb 13, 2010).

Thomas, Timothy L. "Hezballah, Israel, and Cyber Psyop." IO Sphere, Winter 2007: 30-35.

United States Air Force. Air Force Doctrine Document 2-5: Information Operations. Washington DC: Department of Defense, 2005.

United States. Joint Publication 3-13.2: Psychological Operations. Washington DC: Department of Defense, 2010.

—. Joint Publication 3-13.4: Military Deception. Washington DC: Department of Defense, 2006.

—. Joint Publication 3-13: Information Operations. Washington D.C.: Department of Defense, 2006.

—. Joint Publication 3-61: Public Affairs. Washington DC: Department of Defense, 2005.

Wikipedia On-line Encyclopedia. Entry for Propaganda. http://en.wikipedia.org/wiki/Propaganda (accessed January 25, 2010).