NAVAL WAR COLLEGE
Newport, R.I.

WAR.COM:
THE INTERNET AND PSYCHOLOGICAL OPERATIONS

by

Angela Maria Lungu
Major, US Army

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

5 February 2001

_____

CAPTAIN Patrick T. Tooey
Professor, JMO Department

REPORT DOCUMENTATION PAGE

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
05-02-2001	Final Report	xx-xx-2001 to xx-xx-2001

4. TITLE AND SUBTITLE War.com: The Internet and Psychological Operations Unclassified	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Tooney, Patrick H. ;	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME AND ADDRESS Joint Military Operations Department Naval War College 686 Cushing Road Newport , RI 02841-1207	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS ,	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT
A
PUBLIC RELEASE

,

13. SUPPLEMENTARY NOTES

A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

As an information medium and vehicle of influence, the Internet is a powerful tool, in both open societies as well as in those whose only glimpse of the outside world is increasingly viewed and shaped through webpages, E-mail, and electronic chat rooms. Moreover, the sword cuts both ways, as unconstrained (legally, socially, politically) adversaries find the Internet an effective vehicle for influencing popular support for their cause or inciting the opposite against the U.S. or its interests. Consequently, the realm of military psychological operations (PSYOP) must be expanded to include the Internet. Just as obvious is the need for action to remove or update current policy and legal constraints on the use of the Internet by military PSYOP forces, allowing them to embrace the full range of media, so that the U.S. will not be placed at a disadvantage. Although current international law restricts many aspects of PSYOP either through ambiguity or non-currency, there is ample legal room for both the U.S. and others to conduct PSYOP using modern technology and media such as the Internet. Existing policy and legal restrictions, however, must be changed, allowing military PSYOP forces to both defend and counter adversarial disinformation and propaganda attacks which impact on the achievement of military objectives. By examining this issue, I hope to highlight the importance of the Internet for PSYOP and foment further discussion.

15. SUBJECT TERMS

Internet; Psyop; Psychological Operations; Future Warfare; Public Diplomacy; Propaganda; Legal

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Fenster, Lynn lfenster@dtic.mil
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	Public Release	30	**19b. TELEPHONE NUMBER** **International Area Code** **Area Code Telephone Number** 703 767-9007 **DSN** 427-9007

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	**7. Address**: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): WAR.COM: THE INTERNET AND PSYCHOLOGICAL OPERATIONS (UNCLASSIFIED)	
9. Personal Authors: MAJOR ANGELA MARIA LUNGU, US ARMY	
10.Type of Report: FINAL	**11. Date of Report**: 5 FEB 01
12.Page Count: 17	**12A. Paper Advisor (if any):** CAPTAIN PATRICK H. TOOEY
13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: INTERNET, PSYOP, PSYCHOLOGICAL OPERATIONS, FUTURE WARFARE, PUBLIC DIPLOMACY, PROPAGANDA, LEGAL	

15.Abstract:

As an information medium and vehicle of influence, the Internet is a powerful tool, in both open societies as well as in those whose only glimpse of the outside world is increasingly viewed and shaped through webpages, E-mail, and electronic chat rooms. Moreover, the sword cuts both ways, as unconstrained (legally, socially, politically) adversaries find the Internet an effective vehicle for influencing popular support for their cause or inciting the opposite against the U.S. or its interests. Consequently, the realm of military psychological operations (PSYOP) must be expanded to include the Internet.

Just as obvious is the need for action to remove or update current policy and legal constraints on the use of the Internet by military PSYOP forces, allowing them to embrace the full range of media, so that the U.S. will not be placed at a disadvantage. Although current international law restricts many aspects of PSYOP either through ambiguity or non-currency, there is ample legal room for both the U.S. and others to conduct PSYOP using modern technology and media such as the Internet. Existing policy and legal restrictions, however, must be changed, allowing military PSYOP forces to both defend and counter adversarial disinformation and propaganda attacks which impact on the achievement of military objectives. By examining this issue, I hope to highlight the importance of the Internet for PSYOP and foment further discussion.

16.Distribution / Availability of Abstract:	**Unclassified** **X**	**Same As Rpt**	**DTIC Users**
17.Abstract Security Classification: UNCLASSIFIED			
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19.Telephone: 841-6461		**20.Office Symbol:** C	

Security Classification of This Page Unclassified

Abstract

WAR.COM:
THE INTERNET AND PSYCHOLOGICAL OPERATIONS

As an information medium and vehicle of influence, the Internet is a powerful tool, in both open societies as well as in those whose only glimpse of the outside world is increasingly viewed and shaped through webpages, E-mail, and electronic chat rooms. Moreover, the sword cuts both ways, as unconstrained (legally, socially, politically) adversaries find the Internet an effective vehicle for influencing popular support for their cause or inciting the opposite against the U.S. or its interests. Consequently, the realm of military psychological operations (PSYOP) must be expanded to include the Internet.

Just as obvious is the need for action to remove or update current policy and legal constraints on the use of the Internet by military PSYOP forces, allowing them to embrace the full range of media, so that the U.S. will not be placed at a disadvantage. Although current international law restricts many aspects of PSYOP either through ambiguity or non-currency, there is ample legal room for both the U.S. and others to conduct PSYOP using modern technology and media such as the Internet. Existing policy and legal restrictions, however, must be changed, allowing military PSYOP forces to both defend and counter adversarial disinformation and propaganda attacks which impact on the achievement of military objectives. By examining this issue, I hope to highlight the importance of the Internet for PSYOP and foment further discussion.

TABLE OF CONTENTS

Abstract ii
TABLE OF CONTENTS iii
1. INTRODUCTION 1
2. PSYOP AND PUBLIC DIPLOMACY 2
Growing Popularity of PSYOP 2
3. PSYOP AND THE LAW 3
Domestic Law 4
International Law 5
Counterarguments 6
4. PSYOP AND THE INTERNET 7
Internet Proliferation 7
Future Warfare and PSYOP 8
Implications for PSYOP 9
5. PSYOP AND THE FUTURE 14
6. CONCLUSIONS 16
NOTES 18
BIBLIOGRAPHY 24

1. INTRODUCTION

Subcomandante Marcos of the Zapatista National Liberation Army uses a laptop computer amidst the jungles of Chiapas to send carefully written communiqués and appeals to international organizations and journalists, ultimately garnering domestic and international support.[1] Only a few years later and a continent away, a dark-haired girl scowls from the wheelbarrow her father is pushing across the Kosovo border into Albania, in a photo on the U.S. Information Agency's[2] Kosovo website. A few clicks away, on a Serb website, another little girl is seen smiling in a snapshot with the caption: "Brutally killed by NATO a few days before her birthday."[3]

These two vignettes demonstrate a modern twist on von Clausewitz: the Internet as "an increasing continuation of war by other means."[4] This cyberspace "clickskrieg"[5] represents a dramatic shift in strategic thinking regarding national security and changes the ways of looking at warfare. One defense analyst notes "we have to get beyond the notion that warfare is only about hurling mass and energy at our opponents--it's also about hurling information."[6] From the Amazon jungle to Kosovo, new technologies are enabling organizations to use information power to counter or fortify raw power."[7]

As an information medium and vehicle of influence, the Internet is a powerful tool, in both open societies as well as in those whose only glimpse of the outside world is increasingly viewed and shaped through webpages, E-mail, and electronic chat rooms. Moreover, the sword cuts both ways, as unconstrained (legally, socially, and politically) adversaries find the Internet an effective vehicle for influencing popular support for their cause or inciting the opposite against the U.S. or its interests. Consequently, the realm of military psychological operations (PSYOP) must be expanded to include the Internet. By

examining this issue, I hope to highlight the importance of the Internet for PSYOP and foment further discussion.

2. PSYOP AND PUBLIC DIPLOMACY

U.S. public diplomacy plays an important role in national power, as a component of both the diplomatic and informational elements, and military PSYOP can be used to exercise public diplomacy within the scope of military operations (specifically, within a defined operational area outside the U.S.). As defined by Joint Publication 3-53,

> PSYOP are operations planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.[8]

One of the principal missions of PSYOP personnel is to serve as the supported military commander's "voice to foreign populations to convey intent, including political decision-makers, military commanders, forces, and civilian populations, as well as sources of external support."[9] Similarly, public diplomacy is defined as "[promoting] the national interest of the U.S. through understanding, informing and influencing foreign audiences,"[10] sharing the same objective as PSYOP. Moreover, it is critical that all themes and objectives reflect and fully support the U.S. national policy, and national informational programs must integrate Department of Defense (DOD) PSYOP efforts into all international information programs to ensure consistent, non-contradictory messages or information.[11]

Growing Popularity of PSYOP

There is presently a renewed interest in the use of coordinated information programs, military PSYOP in particular, due to three compelling reasons. First, there is a politically driven movement to prevent a potential adversary's escalation towards violent resolution of

differences. Second, due to the Internet and technology, it is almost impossible for governments to regulate the flow of information across their borders, thus making potential target audiences more accessible to PSYOP messages, both friendly and otherwise. Third, the growing world trend towards urbanization, particularly in the third world,[12] coupled with the ubiquitous and scrutinizing international media, makes the use of overwhelming firepower far less palatable in view of large noncombatant populations.

Moreover, especially in the context of actions in Mogadishu and Grozny, these lessons have been learned and applied by potential adversaries of the U.S. In all of these situations, the requirement for U.S. forces to be able to communicate effectively and persuasively with local groups, organizations, and leaders is key to achieving both military and political goals. More importantly, in many cases the "destructiveness of conventional weaponry is too much and diplomacy is not enough," in which case non-lethal weapons such as PSYOP "could be used to fill that gap and at the same time reduce the risk of military overkill, international censure, political repercussions, or media criticism, neatly [fitting] the gap between diplomacy and combat."[13]

3. PSYOP AND THE LAW

Despite this growing interest, there are still significant legal boundaries constraining PSYOP. Currently, both U.S. policy and law prohibit military forces from conducting PSYOP against American citizens,[14] in addition to restrictions imposed by international law. This becomes a crucial point since today's public diplomacy messages are increasingly delivered to both domestic and foreign audiences by many of the same media (CNN, the World Wide Web, and international wire services) and can be accessed on the Internet from anywhere, which in turn have a significant impact on PSYOP forces' dissemination means.[15]

Domestic Law

There are several laws that govern public diplomacy which, because many PSYOP products and their dissemination constitute a form of public diplomacy, also govern military PSYOP. The Smith-Mundt Act[16] was introduced in 1948 as an outgrowth of President Wilson's Committee on Public Information[17] and President Truman's "Campaign of Truth" programs.[18] It was passed unanimously by Congress, becoming the basic charter for postwar public diplomacy policy, and established of the U.S. Information Agency (USIA), whose two-fold mission was to "[project] an accurate image of American society and [explain] to foreign audiences the nature, meaning, and rationale of our foreign policies."[19] The Foreign-Relations Act of 1972 amended the Smith-Mundt Act to include a ban on disseminating within the U.S. any "information about the U.S., its people, and its policies"[20] prepared for dissemination abroad, and the Zorinksy Amendment further restricted public diplomacy by prohibiting any funds to be used "…to influence public opinion in the [U.S.], and no program material … shall be distributed within the [U.S.]."[21] Additionally, the 1998 Foreign Relations Restructuring Act merged several agencies, to include the USIA, under the Department of State (DOS), and authorized the DOS to conduct Foreign Public Diplomacy.[22]

The point of contention rests on the difficulty of sending one message to international audiences while sending another to domestic media, particularly when viewed through the legal lens.[23] The charter of Presidential Decision Directive (PDD) 68, *International Public Information*, focused on this point, making clear that international public information (IPI) activities "are overt and address foreign audiences only," while at the same time noting that domestic information should be "deconflicted" and "synchronized" so as not to send a contradictory message. As one administration official said, "In the old days, the [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. IPI is a mechanism that has been established to make sure that these various actors are working in a coordinated manner."[24]

International Law

In addition to the domestic limitations, there exist international legal barriers to using the Internet for PSYOP. Both explicit regulations of particular actions or more general principles of international law may constrain PSYOP due to the fact that information technology is far newer than existing laws, resulting in ambiguity of what is legally defined as war and an absence of provisions that explicitly prohibit information attacks. Consequently, there exist several areas of contention in the realm of information warfare.[25]

There are several reasons for the difficulty in resolving these issues. While the perpetrators of cyberwar (knowledge-related conflict at the military level) attacks may be formal military forces, netwar (societal struggles most often associated with low intensity conflict) attacks may not even be traditional military forces,[26] but instead may "often involve non-state, paramilitary, and irregular forces."[27] Additionally, it has not been established that information attacks, especially when they are not directly lethal or physically destructive, constitute the use of "force" or "armed attack" under such provisions as the United Nations (U.N.) Charter,[28] and may thus be legal forms of coercion even in peacetime.[29] Distorting enemy perceptions may also be illegal or limited by laws against perfidy.[30]

In spite of the legal constraints, there are many areas of PSYOP that are considered within the realm of international law. For example, the rules of the International

Telecommunication Union do not apply between belligerents, making wartime communications fair game. Specifically relating to PSYOP,

> manipulating enemy perceptions, spreading confusion or disaffection by covertly altering official announcements or news broadcasts, or confusing or frightening leaders by spoofing intelligence or other government communications in principle would not violate the laws of war. However, manipulating an adversary nation to the extent that its citizens or leaders become unhinged from reality, or using propaganda, video morphing, or deceptive broadcasts to the extent that they spur unrestrained civil war or genocide may also be illegal.[31]

Counterarguments

The major arguments against Internet PSYOP primarily concern isolation of target audiences, namely, preventing Americans from viewing Internet products. Using traditional media whose dissemination can be somewhat controlled, target audiences can be pinpointed with relative assuredness. Historically, the use of language as well as geographic ranges and reach of dissemination devices have been the primary means for targeting specific audiences. The changing linguistic demographics within the U.S. (rise of Spanish and other non-English languages) as well as an increasingly global culture and media network (alá Hollywood and CNN) make this approach progressively impractical. The Internet, plainly, is only one (albeit the most obviously least restricted) of many other platforms. Central news services (Associated Press, Reuters), the more economical (yet less diverse) sharing of foreign TV correspondents and bureaus, and a dominant U.S. influence globally ("Americanization") are primarily responsible for this situation. Collectively, these media have a far greater reach and are far less controllable than ever before. Today, the "transmission of data is almost instant, regardless of where sender and receiver are."[32]

Since narrowing the target audience is almost impossible, many of these unintended consequences can be avoided by focusing on dissemination of credible information primarily

in response to adversarial propaganda as well as development of messages appealing to specific groups. Up until its incorporation into the DOS in 1999, for example, the USIS maintained two separate websites: one for American citizens with its USIA title, and the other intended for foreign audiences (under its U.S. Information Service title). Even today, the English language website of the DOS' Office of International Information Programs (formerly USIA) differs from its French and Spanish language websites, primarily in that the non-English sites contain links to articles on human rights (specifically on abuses in Cuba and Peru), drugs, and corruption, as well as reports with such titles as "Towards a Community of Democracies" and "The World AIDS Epidemic," none of which appear on the English site. Of particular note is that both the French and Spanish sites also contain links to the Voice of America site, which by law cannot be broadcast into the U.S. Additional content differences are obviously selected based on regional interest and relevancy. This cursory content analysis is not intended to discredit the DOS, but rather to highlight how they are currently handling the issues of Internet target audiences.

Clearly, current policies have become obsolete and must be reexamined. Without changing the restrictions against specifically targeting American citizens, it is still possible to change existing policies prohibiting the use of the Internet by these forces, thereby enabling them to disseminate relevant and timely products to target audiences best reached through the Internet, as well as to effectively counter propaganda directed against the U.S.

4. PSYOP AND THE INTERNET

Internet Proliferation

The Internet is an important medium for reaching and influencing audiences. Currently, the backbone of the Internet moves information at gigabits per second[33] and involves access

to information through a variety of means, including newsgroups, World Wide Web, E-mail, gopher, Telnet, file transfer protocol, and Internet relay chat. There are currently 375 million Internet users worldwide (36% in the U.S.), growing to 840 million by 2005 and over 1.8 billion by 2010.[34] Between 2002 and 2005, broadband connections, web cellular phones, web entertainment appliances, and web interactive TV service will be among the most important factors driving the growth of the Internet.[35] The next generation cellular technology (3G) may be the biggest broadband of them all and is estimated to be deployed in Japan and Europe two years ahead of the U.S., extending the number of web users (with web cellular phones), most notably in developing countries where fixed phone lines are limited.[36] These factors are particularly relevant since greater multimedia content can be transferred to a greater number of people, especially in previously inaccessible regions, with larger audiences being influenced by Internet media.

Future Warfare and PSYOP

Increasingly, information technology rather than traditional military means will be the preferred method of attacking U.S. interests, attempting to "manipulate policy- and decision-makers by attacking our information infrastructure through selected, discriminate releases via both legitimate news organs and nontraditional means."[37] This can be accomplished in a variety of ways, as the President's Commission on Critical Infrastructure Protection describes:

> Offensive information warfare is attractive to any because it is cheap in relation to the cost of developing, maintaining, and using advanced military capabilities. It may cost little to suborn [bribe] an insider, create false information, [or] manipulate information….against an information system connected to the globally shared information infrastructure.[38]

This theme was further expanded in a prescient 1989 *Marine Gazette* article examining the evolution of warfare, which predicted that in the "fourth generation" the battlefield would

> envelop entire societies….and military objectives would no longer involve annihilating tidy enemy lines, but rather eroding popular support for the war within the enemy's society….collapsing the enemy internally rather than physically destroying him.[39]

Although the Internet was not yet a driving force in 1989, the authors warned that highly sophisticated PSYOP might become the "dominant operational and strategic weapon in the form of media/information intervention…especially through manipulation of the media."[40] What is alarming is that, against this non-traditional warfare, "a lot of capabilities we have just simply aren't relevant," says Michael G. Vickers, director of strategic studies at the Center for Strategic and Budgetary Assessments.[41]

Implications for PSYOP

There is without a doubt a growing relevance of the Internet as a medium for not only information, but as a means of reaching and influencing decision-makers and their constituencies. According to a senior defense analyst, today's battle-space is people's minds, with the criteria for winning or losing heavily culture-dependent. Weapons of mass destruction are "weapons of mass *disruption*," and the combat zones are now Usenet newsgroups.[42] "The consumer's center of gravity is rapidly shifting to the Internet; broadcasting is no longer how the media works," continues a recent Defense Science Board report, and radio and TV transmissions are increasingly irrelevant in molding public opinion.[43] Today, in order to remain relevant,

> PSYOP must demonstrably influence audiences in an increasingly sophisticated international information environment…Without a fundamental change in the way PSYOP forces are permitted to conduct day-to-day functions, they can never co-opt the information cycle of a sophisticated adversary such as the indigenous media in Bosnia.[44]

The Internet, as an increasingly more potent influence medium, is also an increasingly more relevant PSYOP tool.

The capabilities of the Internet as a medium for PSYOP are further enhanced when viewed in terms of audience and objectives. State and non-state actors are increasingly turning to the Internet as a means for garnering domestic and international support and approval, which in turn helps legitimize the issue among international organizations. As the executive agency for the 1997 Dayton Accord, for example, the Organization for Security and Co-operation in Europe (OSCE) used the Internet to complement more conventional public information and voter information efforts as a means of reinforcing its legitimacy as an international organization, while also gaining continued support.[45] It is of particular interest in how the Internet was used to indirectly distribute information to both local and international media, as recounted by Peter Clarey, OSCE Public Information Officer:

> 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.[46]

Going beyond simply providing information, the Mexican Zapatistas also used this technique, as did the Serbs and Kosovars in what has been described as the first online war in which both sides used websites and E-mail lists to "make their case, to set goals, retell histories, and make stands."[47] As information operations[48] become more popular and more refined, it is apparent that instead of simple denial-of-service,

> Information operations should increasingly be about affecting the perceptions, and thus the resultant behavior, of a selected human target set…done by manipulating the information available to the target so that, in a given situation, the behavior we desire on the part of the target will occur.[49]

Potential adversaries recognize this as well, and Arquilla and Ronfeldt note, "Protagonists are more interested in keeping the Net up than taking it down, so they can use it to mobilize their forces, disseminate their views, and try to affect the beliefs and opinions of other people."[50]

After NATO bombed Serb media outlets considered a source of Milosevic propaganda, for example, the U.S. government decided not to cut off Serb Internet sites. DOS spokesman James Rubin responded, "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."[51] However, as noted by many analysts and commanders, at the start of the conflict, Serbia maintained information superiority over the minds of its citizens and, to a lesser extent, outside Serbia. Admiral Ellis, Commander-in-Chief of NATO's Allied Forces Southern Europe, recounted not being able to counter Milosevic's state-controlled media or his attempts to gain international sympathy, as well as having to respond to NATO's collateral damage problem while Milosevic's forces killed hundreds of people.[52] The Serbs also used the Internet to spread various campaign themes, causing the USIA to expend great efforts to control the fallout effects on U.S. credibility.[53] In this way, Milosevic was able to asymmetrically respond to U.S. and NATO actions.

Yet another implication is the changing dynamic of how the media sees and reports on conflicts, which is significantly affected by the interactivity of the Internet. "[Talking] to the enemy without the intervention of propaganda or governments" during the NATO bombing of Serbia via E-mail and chat rooms, for example, evoked interesting responses from media leaders. The international editor of the MSNBC.com site maintained an ongoing

conversation with about 36 Serbs and stated that it was a revelation for him "to see how it has given people on both sides of this struggle incredible access to news decision makers."[54] According to the New York editor of the online magazine *Slate*, who published the diary of a *Slate* correspondent in Belgrade during the bombing, "It does change the terms of the engagement. It is very democratizing. It makes it much more difficult to demonize the enemy."[55] In this way, the more traditional media is being ever more influenced by online media and "non-journalists, often with a personal interest in how the war if fought and how it ends,"[56] ultimately impacting public opinion and decision-makers at the highest levels.

Rather than exploit the Internet through webpage content, however, some countries attempt to restrict or control access to the Internet in order to reduce or eliminate the influence of controversial or adversarial groups. In China, the Ministry of State Security shut down the website of the New Culture Forum, accusing the group of posting "counter-revolutionary content," the latest of a supposedly ongoing attempt to contain "the spread of political dissidence and pornography on the Internet."[57] This was quickly followed by a call to arms by the *People's Daily* in Beijing against enemy forces at home and abroad that use the Internet as a "battlefront to infiltrate" China. China employs other tactics as well, such as blocking undesirable websites to limit release of information from China-based Internet content providers, and has also deliberately slowed down Internet traffic on its international routes.[58] The country has expended vast resources to contain its perceived "Internet threat," helping to earn China the title of one of the 20 enemies of the Internet in 1999.[59]

Interestingly, the Chinese government, recognizing the role of the Internet, has invested a great deal in establishing a national telecom infrastructure (China Telecom), a Government Online Project (bringing government agencies to the Internet), and a similar Enterprise

Online Project for Chinese industry. Through these initiatives and America Online-type promotions, China, although an Internet latecomer, is now fifth in international rankings of Internet users, with a 4.2% share (ahead of Canada, South Korea, France, and Australia).[60] It is clear that this is a coherent and targeted strategy, as Major General Wang Pufeng outlined, "In situations of information defense, we must strive for an active approach in a reactive situation and use every means possible to destroy the opponent's information superiority and transform our inferior position in information."[61]

Other examples of restricting the Internet include Britain's Regulation of Investigatory Powers Act that gives its police sweeping access to E-mail and other online communications, the outlaw of access to gambling websites in South Korea, and even the U.S. law requiring computer filtering software in federally funded schools and libraries to "block material harmful to the young."[62] Most recently notable has been the French ruling against Yahoo! that ordered the company to either find some way to prevent French users from seeing the Nazi memorabilia posted on its American sites or else pay a daily fine of FFr100,000.[63]

A government can also use the Internet to censor.[64] Singapore began attempts to censor the Internet, and other Asian countries such as Vietnam, China, Indonesia, and Malaysia soon followed suit. Russia attempted to remove the Chechen site from a U.S. server by launching a diplomatic offensive just before the Russian attack on Chechnya, and the U.S. server complied, saying the Chechen site contained terrorist propaganda and hate material.[65] Censoring is only temporary, though, since the affected group or organization can quickly find a publicly accessible news server that carries the censored newsgroup (e.g., via webpage or E-mail); take out an account with an Internet service provider (ISP) in a different country; or employ third parties to send and receive newsgroup contributions.[66]

When the Serb government cut off the independent radio station B92, for example, which was being used to coordinate protest demonstrations over the Milosevic government's refusal to accept the local election results, the leaders of the demonstrations rerouted B92's broadcasts to the Internet, whose Real Audio transmissions were then picked up by Voice of America and the British Broadcasting Corporation in the Netherlands and rebroadcast back into Serbia – thus allowing the demonstrators to continue. Radio Belgrade similarly rerouted their broadcasts after NATO bombing of their radio stations through Germany.[67]

Whether used offensively or defensively, it is clear that the Internet is an important tool for PSYOP and can bring tremendous capabilities and informational advantage to forces employing this medium. It is easy to see that "the most powerful state or entity will be the one that controls and manages information the most effectively."[68]

5. PSYOP AND THE FUTURE

Given the strategic opportunities afforded by the Internet, there are several options for employing this medium. DOD, in particular, could use the Internet offensively to help achieve unconventional warfare objectives, as well as to address and counter adversarial propaganda, disinformation, and neutral party information.

During the Kosovo crisis, former-USIA chief information officer Jonathan Spalter stated, "the measure of [USIA's] success is the extent to which we are perceived not as propaganda but anti-propaganda."[69] In addition to websites, pre-empting messages and developing Internet products such as streaming audio/video, online video games, mediated newsgroups, and ad banners can also be leveraged for their strategic value and reach. The recent Defense Science Board report on PSYOP also suggested some less obvious potential tools using emerging media technologies, such as chat rooms and instant messaging services

that could be used for "guided discussions" to influence how citizens thinks about certain topics," and even noted that both U.S. presidential candidates and the Chinese government have used similar Internet technologies for information dissemination.[70]

Information could also be transmitted over the Internet to sympathetic groups operating in areas of concern that allow them to conduct operations themselves that the U.S. might otherwise have to send its own special forces to accomplish."[71] During conflict, the Internet is invaluable for getting news out of the region and into the U.S. government, getting information from the U.S. and other nations into the region, and cultivating political (and even operational) support for the U.S. side and opposition to the other side.[72] Because journalists may not always have access to the crisis locations, they may also rely on Internet sites for information, which serves to further multiply the effectiveness of whatever side was able to get its story out.

The crises in Kosovo as well as in Chechnya are two good examples. Both the Serb government (www.serbia-info.com) and the Kosova Liberation Army (KLA) (www.kosova.com) are using websites and e-mail lists to make their case, with both sides competing for international support. The Serb and KLA sites report daily events that "differ so completely they seem to come from separate planets."[73] In January 1999, the KLA posted disturbingly graphic photos of what they claim to be the Racak Massacre, while the Serbs offer reports from an Italian journal and French newspapers (*Le Figaro, Le Monde*) that offer "proof" that there was no massacre in Racak – that it was a setup.[74]

The Chechen site (kavkaz.org), run by the former Chechen information minister, takes lessons from the Serbs and features footage of Russia's bombing and shelling campaign.

> [Putin] flatly denied…that Russian tanks had fired on a bus in northeastern Chechnya…killing dozens of civilians. But the Chechens had already posted

> photographs on the Internet showing a bus shot to pieces and the mangled corpses of several female passengers.[75]

As a result, then-Prime Minister Putin launched the Russian Information Center (RIC) (http://www.gov.ru/) to combat the Chechen site, putting out only Russian government information, and limited access to the region by journalists. After losing the propaganda war in 1994-96, senior Russian strategists developed a concentrated media plan (using the RIC) to target Russian popular support for Moscow's actions during the second Chechen war. The results have been dramatic, with a complete reversal in the ratio of Russians who support military force in Chechnya.[76]

The Internet can also be used as a defensive technique, primarily guarding against defacement of official websites and databases. Filtering and blocking software can be installed on individual computers, at an ISP, or on country gateways linking to the rest of the world, and websites themselves can block users based on the user's Internet protocol address, which can identify particular computers as well as their locations.[77] Acting more offensively, PSYOP forces could use the Internet to address and counter adversarial propaganda, disinformation, and neutral party information.[78]

6. CONCLUSIONS

"No law can change as swiftly as can technology; unless law is to somehow stop technology's seemingly inexorable worldwide progress, it cannot fully control the use of its fruits for warfare."[79] It is clear that the Internet is a potentially valuable medium for PSYOP given the trends in today's world, and increasing numbers of state and non-state actors are taking full advantage of this opportunity. The Internet is an inevitable extension of today's battlefield and using this medium for psychological operations during war is a critical capability that must be employed. Just as obvious is the need for action to remove or update

current policy and legal constraints on the use of the Internet by military PSYOP forces, allowing them to embrace the full range of contemporary media and not place the U.S. at a disadvantage in future conflicts. It is critical that U.S. decision-makers balance offensive opportunities against defensive vulnerabilities when considering policy options.[80]

Although current international law restricts many aspects of PSYOP either through ambiguity or non-currency, there is ample legal room for both the U.S. and others (like the double edged sword, it can cut both ways) to conduct PSYOP using modern technology and media such as the Internet. Current policy and legal restrictions, however, must be changed, allowing military PSYOP forces to both defend and counter adversarial disinformation and propaganda attacks which impact on the achievement of military objectives. As warned by the Defense Science Board, "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."[81]

It is therefore necessary for the DOD to address PSYOP use of the Internet "directly and explicitly as an integral asset," instead of as an "uncontrollable element of the environment whose role is determined by happenstance or as an afterthought in order to use it in the most productive manner possible. Furthermore, "if viewed as a resource and systematically integrated into U.S. planning and operations, the Internet can make some important contributions to conflict management and assuring the success of U.S. foreign policy."[82] "Bombs and missiles will still determine who militarily wins or loses a conflict…PSYOPS [sic], though, will help determine how long a conflict lasts and the impact of a military struggle on long-term U.S. strategic interests."[83]

NOTES

[1] Angela Maria Giordano, "Study of a Storm: An Analysis of Zapatista Propaganda," (Unpublished Master's Thesis, U.S. Naval Postgraduate School, Monterey, CA: 1997).

[2] The U.S. Information Agency was reorganized into the International Information Programs Department within the Department of State on 1 October 1999 as part of the Department of State Reorganization Act.

[3] David Briscoe, "Like Air War, Propaganda War Over Kosovo Has No Clear Winner," *The Associated Press*, 17 May 1999: in Eden-Webster Passports/Lexis-Nexis [database online], World News library, (7 January 2001).

[4] Rod Nordland, "War: E-Zone Combat: Hostilities May End On The Battlefield, But There's Never A Truce On The Internet," *Newsweek International* (11 October 1999): 72: in Eden-Webster Passports/Expanded Academic ASAP [database online], #A56023026, (7 January 2001).

[5] Michael Satchell, "Captain Dragan's Serbian Cybercorps (Serbs Used Internet For Propaganda, While NATO Drops Leaflets)," *U.S. News & World Report* 126 (10 May 1999): 42: in Eden-Webster Passports/Expanded Academic ASAP [database online], #A54575536, (7 January 2001).

[6] John Arquilla, as quoted in Lloyd Robertson, "Waging War On The World Wide Web," *CTV Television National News* (Pleasanton, CA: Community Television, 31 March 1999): in Eden-Webster Passports/Lexis-Nexis [transcript online], World News library, (7 January 2001).

[7] David J.Rothkopf, "Cyberpolitik: The Changing Nature Of Power In The Information Age," *Journal of International Affairs* 51 (1998, Spring): in Columbia International Affairs Online [database online], (7 January 2001).

[8] Joint Chiefs of Staff, *Joint Psychological Operations*, Joint Pub 3-53 (Washington, D.C.: GPO, 10 July 1996), I-1.

[9] Department of the Army, *Psychological Operations*, FM 3-05.30 (Washington, D.C.: GPO, 19 June 2000), 1-2 through 1-3, and 1-6.

[10] According to the Planning Group for Integration of USIA into the Department of State. From "What is Public Diplomacy?" (20 June 1997), <http://www.publicdiplomacy.org/1.htm> [28 December 2000]. Public diplomacy also differs from public affairs, whose purpose is primarily to inform domestic audiences, and from traditional diplomacy, in that public diplomacy deals largely with non-governmental organizations and individuals, in addition to government representatives.

[11] This need for unity of effort and unity of themes has long been recognized as critical to the success of any PSYOP plan and is procedurally outlined in President Clinton's Presidential Decision Directive 68, "International Public Information" (30 April 1999). PDD 68 established a standing international public information (IPI) sub-group that works to coordinate and deconflict international information initiatives of the various government agencies (CIA, FBI, and State, Treasury, Commerce, Justice, and Defense departments). Additionally, military PSYOP activity was specifically addressed under this sub-group, and within the interagency arena it is to be called international military information (IMI). This interagency mechanism was designed to coordinate more rapidly and thoroughly on regional plans and programs, and is working to develop a national IPI strategy supportive of the National Security Strategy. From Tom Timmes, OASD-SO/LIC (Policy Planning), <timmest@mail.policy.osd.mil> "Re: PDD68," [E-mail to author <lungua@soc.mil>] June 9, 1999. Specifically, the IPI sub-group will design information campaigns to support policy initiatives and submit them to the Deputies Committee or Principals Committee for approval and implementation by the various agencies, thus providing the policy framework and directive authority necessary for mutually supportive works and deeds on a truly strategic level. From Charles A.Williamson, "Psychological Operations In The

Information Age," in *Cyberwar 2.0: Myths, Mysteries and Reality,* edited by Alan D. Campen and Douglas H. Dearth (Fairfax, VA: AFCEA International Press, 1998), 179-189.

[12] Given current population trends, by 2015, 24 of 27 cities with over a 10 million population will be in the Third World and almost 70% of the world's population will be urban. From United Nations, Population Division, *World Urbanization Prospects: The 1994 Revision* (1995), as quoted in Tom Bowman, "War Games In NC Prepare Marines For The 21st Century," *Baltimore Sun*, 28 December 1997, <http://newslibrary.krmediastream.com/cgi-bin/search/bs> [7 January 2001].

[13] David Shukman, *Tomorrow's War: The Threat of High-Technology Weapons* (New York: Harcourt Brace & Company, 1996), 220 and 227.

[14] The use of military PSYOP equipment and personnel, however, has been allowed during times of national emergency for assisting other lead U.S. agencies with the dissemination of public safety and health information, such as during Hurricane Andrew in the Southeast U.S. in August, 1992.

[15] Military PSYOP forces are assigned to the U.S. Special Operations Command, and are largely found in the Army. The other Services have limited PSYOP resources, such as the Air Force's EC-130 "Commando Solo" aircraft, the Navy's Fleet Information Warfare Center, and the Marine Reserve Civil Affairs Group (which have small PSYOP units to advise on PSYOP). Additionally, approximately three quarters of the Army PSYOP forces are in the Reserve.

[16] The official title was the United States International Information and Educational Exchange Act of 1948 (Public Law 80-402), but is better known and referenced simply as the Smith-Mundt Act of 1948.

[17] This was American's first official government propaganda program that "sold" the American public on entering the First World War. The stated task was to inform and influence the world at large, including American citizens, about the democratic goals of U.S. policy and the threat t the world of the imperialistic goals of the enemy states, especially the German Empire." See John S. Gibson, "Public Diplomacy,"*International Educator* VII *(*Spring 1998) from Debra Weltz, <weltzd@soc.mil> "Re: Research," [E-mail to author <angelamaria@lungu.com>] 14 December 2000.

[18] This program was designed to counter Soviet propaganda. From Dr. Nancy Snow, "The Smith-Mundt Act of 1948: A Fifty-year Legacy of U.S. Propaganda," an abridged version from Debra Weltz, <weltzd@soc.mil> "Re: Research," [E-mail to author <angelamaria@lungu.com>] 14 December 2000. The article originally appeared *in Propaganda, Inc.: Selling America's Culture to the World* (Seven Stories Press), and later appeared as "The Smith Mundt Act of 1948" in *Peace Review* 10 (December 1998).

[19] According to then-Director Charles Z. Wick, as quoted in Gibson.

[20] President William J. Clinton, "Reorganization Plan and Report to the Congress" (regarding the Foreign Affairs Reform and Restructuring Act of 1998), 30 December 1998, <http://fas.org/irp/offdocs/pdd/pdd-68-dos.htm> [5 January 2001].

[21] Ibid.

[22] The DOS Office of International Information Programs (IIP) is now the principal international strategic communications service for the foreign affairs community, developing and implementing "information initiatives and strategic communications programs," to include Internet publications and websites. See Department of State, "About the Office of International Information Programs," <http://usinfo.state.gov/abtusia/aboutiip.htm> [5 January 2001]. Furthermore, in her confirmation hearing statement, Undersecretary of State for Public Diplomacy and Public Affairs Evelyn Lieberman testified to the role of new media technologies in the realm of public diplomacy and the growing list of participants in foreign relations, which includes non-government organizations, multi-national corporations, private nonprofit organization, foundations, and

cultural, educational and advocacy groups. She noted, "In the world of the Internet and satellite television, policy-makers are less and less able to make decisions behind closed doors." From Evelyn S. Lieberman, "Confirmation Hearing Statement," U.S. Congress, Senate Foreign Relations Committee (27 July 1999) <http://www.state.gov/www/about_state/biography/990727_lieberman_conf.html> [5 January 2001].

[23] See Science Applications International Corporation (SAIC), *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance* (Washington, D.C.: SAIC, 4 July 1995) for discussion of these legal issues and the potential conflict between individual liberties (including freedom of expression under the First Amendment) and national security.

[24] Ben Barber, "Group will battle propaganda abroad," *The Washington Times*, 28 July 1999, in Northern Light [database online], (7 January 2001).

[25] There are four main areas. First, there is the difficulty distinguishing between intended targets as military (and thus general legitimate targets) or civilian (generally forbidden), and the issues of secondary and tertiary order effects only serve to compound this idea. Second, the intangible nature of damages from information attacks may be analytically different from the physical damage caused by traditional warfare. Third, the concepts of national, territorial sovereignty take on new meaning in terms of the nature of information and the Internet to travel across international networks or through the atmosphere as radio waves. Finally, the injuries resulting from information warfare attacks may not be the same as described in existing humanitarian law for protection noncombatants. In Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, *Information Warfare and International Law* (Washington, D.C.: DOD Command and Control Research Program, National Defense University, 1998), 10-11.

[26] It is estimated that 95% of the telecommunications of the DOD travel through the Public Switched Network. In Richard W. Aldrich, "The International Legal Implications of Information Warfare" (Occasional Paper 9), *U.S. Air Force Institute for National Security Studies* (Colorado Springs: U.S. Air Force Institute for National Security Studies, April 1999), 3. As Vice Admiral ArthurCebrowski observed, "There is no logical distinction between military or civil systems or technologies…[Therefore] there is also no technical distinction between exploitation, attack or defense of the information warfare target set." In "Information Revolution Spawns 'Revolution in Security Affairs," *Defense Daily* (Washington, D.C., GPO, 8 June 1995).

[27] John Arquilla and David Ronfeldt, "A New Epoch—and Spectrum—of Conflict," in John Arquilla and David Ronfeldt, ed., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997), <http://www.rand.org/publications/ MR/MR880/MR880.ch1.html> [3 April 2000].

[28] Article 51 of the U.N. Charter allows for unilateral retaliation in kind "if an armed attack occurs against a Member of the U.N.," while Article 41 discusses "measures not involving the use of armed force," such as economic relations. From Charles J. Dunlap, Jr., "The Law Of Cyberwar: A Case Study From The Future," in Campen and Dearth, 139-150.

[29] The U.N. Charter does not explicitly define "armed attacks," nor has the International Court of Justice outlined a comprehensive definition. The elements of armed forces, force, violence, and interference with a nation's sovereign rights appear to be elements, yet neither economic coercion nor cumulative guerrilla and terrorist attacks have been recognized as an "armed attack" (Greenberg, Goodman, and Soo Hoo, xvii and 84). If the manipulation of data, however, directly results in "significant destructive effects that are indistinguishable in any meaningful way from those caused by traditional (kinetic) weapons," then those actions would constitute an "armed attack" under Article 51 of the U.N. Charter (Dunlap, 140-142).

[30] Examples include making an adversary believe U.S. troops are surrendering or that combat vehicles were medical vehicles, or manipulating identification signals so that a nation's forces believe that the approaching enemy personnel are actually friendly forces. See Greenberg, Goodman, and Soo Hoo, 35-37.

[31] Ibid.

[32] "Special: The Internet and the Law: Stop Signs on the Web," *The Economist* (11 January 2001), < http://www.economist.com> [15 January 2001].

[33] This is roughly the equivalent of sending the entire Library of Congress (if it were digitized) over the Internet in one minute. From Kurt Mills, *Cybernations: The Internet, Virtual Reality, and Self-Determination*, conference proceedings at the International Studies Association (location not given) (17-21 March 1998): in Columbia International Affairs Online [database online], (7 January 2001).

[34] ETForecasts, "Internet User Forecast by Country," (7 May 2000) <http://www.etforecasts.com/products/ES-intusers.htm> [9 January 2001]. Furthermore, the goal of the European Union'seEurope Action Plan (June 2000) is to close the current Internet gap between the U.S. and Europe, dramatically increasing the current levels of household Internet access in Europe (22% today). FromAri-Veikko Anttiroiko, "Toward European Information Society," *Communications of the Association for Computing Machinery* (January 2001): in Proquest [database online], UMI, (7 January 2001).

[35] Ibid.

[36] Ibid.

[37] Paul R.M.Brooks, Jr. "A vision for PSYOP in the information age." *Special Warfare* 13 (Winter 2000): 20.

[38] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, Robert T. Marsh, Chairman (Washington, D.C.: GPO, October 1997), < http://www.info-sec.com/pccip/ pccip2/report_index.html> [28 December 2000].

[39] William S. Lind and others, "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette* (October 1989): 23.

[40] Ibid., 24, 26.

[41] Stan Crock, "Commentary: Sticks and Stones Can Break an Army," *Business Week Online*" (27 October 2000), from James M. Winters, <jim.winters@monroe.army.mil> "FWD: News: Sticks and Stones Can Break an Army," [E-mail to author <angelamaria@lungu.com>] 27 October 2000.

[42] E. Anders Eriksson, "Information Warfare: Hype or Reality?" *Center for Nonproliferation Studies: The Nonproliferation Review* VI (Spring-Summer 1999): in Columbia International Affairs Online [database online], (28 December 2000). Usenet groups are electronic bulletin boards, and make up a section of the Internet with tens of thousands of newsgroups arranged around special-interest subjects, such as human rights and the environment.

[43] Defense Science Board, *The Creation and Dissemination of All Forms of Information in Support of Psychological Operations in Time of Military Conflict* (Washington, D.C.: GPO, May 2000), 23.

[44] Steve Collins, "Army PSYOP in Bosnia: Capabilities and Constraints," *Parameters* 29 (Summer 1999): 57.

[45] Debra Weltz, Senior Doctrine Writer, PSYOP Division, U.S. Army John F. Kennedy Special Warfare Center and School, <weltzd@soc.mil> "RE: Law Reviews, Combined Smith-Mundt," [E-mail to author <angelamaria@lungu.com>] 14 December 2000.

[46] It was also estimated that only 25,000 homes in BiH (out of approximately 3.5 million) had Internet access. From Peter Clarey, OSCE Public Information Officer, <PeterC@OSCEBIH.org> "Re: Research Question – Elections and the Internet in BiH [what do you think?]," [E-mail to author <lungua@nwc.navy.mil>] 30 January 2001.

[47] Vesna Peric-Zimonjic, "Media-Yugoslavia: Kosovo Combatants Fight New War – In Cyberspace," *World News* (7 August 1998), <http://www.oneworld.org/ips2/aug98/12_15_039.html> [10 December 2000].

[48] PSYOP is one of six capabilities of information operations, which also include deception, physical destruction, electronic warfare, operations security and computer network attack. Civil affairs and public affairs are the two related activities. From Joint Chiefs of Staff, *Information Operations*, Joint Pub 3-13 (Washington, D.C.: GPO, 9 October 1998).

[49] Williamson, 181.

[50] Arquilla and Ronfeldt.

[51] Briscoe; Jon Swartz, "Administration Drops Idea of Blocking Serb Net Sites," *The San Francisco Chronicle*, 15 May 1999: in Eden-Webster Passports/Lexis-Nexis [database online], World News library, (27 December 2000).

[52] Timothy L Thomas, "Kosovo and the Current Myth of Information Superiority," *Parameters* (Spring 2000), <http://carlisle-www.army.mil/usawc/Parameters/00spring/thomas.htm> [16 December 2000].

[53] Ibid.

[54] Tom Regan, "Web War," *Christian Science Monitor*, 22 April 1999, <http://www.csmonitor.com/atcsmonitor/commop/regan/p-regan042299.html> [18 December 2000].

[55] Ibid.

[56] Ibid.

[57] Dali L. Yang, "The Great Net of China," *Harvard International Review* (Winter 2001): in Proquest [database online], UMI, (10 January 2001).

[58] Ibid.

[59] According to the Paris-based *Reporters Sans Frontiers*, as quoted in Yang.

[60] eTForecasts.

[61] Major General Wang Pufeng, "The Challenge of Information Warfare," *China Military Science* (Spring 1995), in "Chinese Intelligence-Related Documents," *Federation of American Scientists*, <http://ftp.fas.org/irp/world/china/ docs/iw_mg_wang.htm> [8 January 2001].

[62] *The Economist*.

[63] This is approximately $13,000. Ibid.

[64] This can be done by applying pressure to an Internet service provider (ISP) to shut down a user or newsgroup; by gaining the cooperation of domestic ISPs, other local telecommunications providers, and/or administrators of computing services within organizations such as a university; or by blocking access to a particular server using software designed to block general access to specified material (e.g., Surf Watch or Cyber Sentry).

[65] Askold Krushelnycky, "Chechnya: Rebels Use Internet in Propaganda War with Russians," *Radio Free Europe/Radio Liberty* (11 May 2000), <http://www.rferl.org/nca/features/2000> [18 December 2000].

[66] Gary Rodan, "The Internet and Political Control in Singapore," *Political Science Quarterly* 113 (Spring 1998): in Columbia International Affairs Online [database online], (9 January 2001).

[67] David J. Rothkopf, " Cyberpolitik: The Changing Nature of Power in the Information Age," *Journal of International Affairs* 51 (Spring 1998): in Columbia International Affairs Online [database online], (9 January 2001).

[68] Brooks.

[69] Briscoe.

[70] Defense Science Board, *Information in Support of Psychological Operations*; Dupont.

[71] Charles Swett, Assistant for Strategic Assessment, Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, Policy Planning, "Strategic Assessment: The Internet," *Federation of American Scientists* (17 July1995), <http://www.fas.org/cp/swett.html> [5 December 2000].

[72] Ibid.

[73] Anne Thompson, "Spin Control: InKosovo's Capital, the War Is All About Words with Yugoslavia," *The Associated Press*, 8 August 1998: in Eden-Webster Passports/Lexis-Nexis [database online], World News library, (7 January 2001).

[74] Renaud Girard, "Kosovo: Obscure Areas of a Massacre," *Le Figaro* (20 January 1999); Christophe Chatelot, "Were the Racak Dead Really Coldly Massacred?" *Le Monde* (21 January 1999). Translations of both articles can be found at International Action Center, "Press Review from DianaJohnstone in Paris," <http://www.iacenter.org/racak.htm>.

[75] Robyn Dixon, "Chechens Use Net in Publicity War with Russia; Putin, Meanwhile, Launches Information Center That Reports Only the Kremlin's Take on Conflict," *Los Angeles Times*, 8 October 1999: in Eden-Webster Passports/Lexis-Nexis [database online], World News library, (3 December 2000).

[76] Emil Pain, "The Second Chechen War: The Information Component," translated by Robert R. Love, *Military Review* (July-August 2000), <http://www.cgsc.army.mil/MilRev/English/JulAug00/love.htm> [3 December 2000].

[77] *The Economist.*

[78] Additionally, due to the "stigma attached to information attacks," which includes PSYOP, many senior information warfare (IW) planners in Washington feel that IW should be "normalized with strict Rules of Engagement," thereby allowing it to be employed like any other weapon system. From Christopher D.Boeting, "Brain Storming," *Jane's Defence Weekly* (16 August 2000), from James M. Winters, <jim.winters@ monroe.army.mil> "FWD: AF IO article," [E-mail to author <angelamaria@lungu.com>] 16 August 2000.

[79] Greenberg, Goodman, and Soo Hoo, 103.

[80] Ibid., xviii.

[81] Defense Science Board, *Information in Support of Psychological Operations.*

[82] Swett.

[83] Defense Science Board, *Information in Support of Psychological Operations.*

BIBLIOGRAPHY

Boeting, Christopher D. "Brain Storming." *Jane's Defence Weekly*. (16 August 2000).

Briscoe, David. "Like Air War, Propaganda War Over Kosovo Has No Clear Winner." *The Associated Press*, 17 May 1999. Eden-Webster Passports/Lexis-Nexis [database online]. World News library. (7 January 2001)

Brooks, Paul R.M., Jr. "A vision for PSYOP in the information age." *Special Warfare* 13 (Winter 2000): 20-24.

Clarey, Peter. OSCE Public Information Officer. <PeterC@OSCEBIH.org> "Re: Research Question – Elections and the Internet in BiH [what do you think?]." [E-mail to author <lungua@nwc.navy.mil>] 30 January 2001.

Clinton, President William J. "Reorganization Plan and Report to the Congress" (regarding the Foreign Affairs Reform and Restructuring Act of 1998). 30 December 1998. <http://fas.org/irp/offdocs/pdd/pdd-68-dos.htm> [5 January 2001].

Collins, Steve. "Army PSYOP in Bosnia: Capabilities and Constraints." *Parameters* 29 (Summer 1999): 57-73.

Crock, Stan. "Commentary: Sticks and Stones Can Break an Army." *Business Week Online.* 27 October 2000. < http://www.businessweek.com/bwdaily/dnflash/oct2000/nf20001027_861.htm> [5 December 2000].

Campen, Alan D. and Douglas H. Dearth, eds. *Cyberwar 2.0: Myths, Mysteries and Reality* (Fairfax, VA: AFCEA International Press, 1998).

Dupont, Daniel G. "Outdated Equipment, Organizational Issues Hamper Effective PSYOPS." *Inside the Pentagon* 5 (28 September 2000).

Eriksson, E. Anders. "Information Warfare: Hype or Reality?" *Center for Nonproliferation Studies: The Nonproliferation Review* VI (Spring-Summer 1999). Columbia International Affairs Online [database online]. (28 December 2000)

ETForecasts. "Internet User Forecast by Country." 7 May 2000. <http://www.etforecasts.com/products/ES-intusers.htm> [9 January 2001].

Gibson, John S. "Public Diplomacy." *International Educator* VII *(*Spring 1998).

Giordano, Angela Maria. "Study of a Storm: An Analysis of Zapatista Propaganda." Unpublished Master's Thesis, U.S. Naval Postgraduate School, Monterey, CA: 1997.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. *Information Warfare and International Law* (Washington, D.C.: DOD Command and Control Research Program. National Defense University, 1998).

Krushelnycky, Askold. "Chechnya: Rebels Use Internet in Propaganda War with Russians." *Radio Free Europe/Radio Liberty.* 11 May 2000. <http://www.rferl.org/nca/features/2000> [18 December 2000].

Lind, William S. and others. "The Changing Face of War: Into the Fourth Generation." *Marine Corps Gazette.* October 1989: 22-26.

Milam, Thomas A, Jr. Deputy Director. U.S. Army John F. Kennedy Special Warfare Center and School. <milamt@soc.mil> "RE: Research Questions." [E-mail to author <angelamaria@lungu.com>] 14 December 2000.

Nordland, Rod. "War: E-Zone Combat: Hostilities May End On The Battlefield, But There's Never A Truce On The Internet." *Newsweek International* (11 October 1999). Eden-Webster Passports/Expanded Academic ASAP [database online]. #A56023026. (7 January 2001)

Pain, Emil. "The Second Chechen War: The Information Component." Translated by Robert R. Love. *Military Review* (July-August 2000). <http://www.cgsc.army.mil/MilRev/English/ JulAug00/love.htm> [3 December 2000].

Peric-Zimonjic, Vesna. "Media-Yugoslavia: Kosovo Combatants Fight New War – In Cyberspace." *World News.* 7 August 1998. <http://www.oneworld.org/ips2/aug98/ 12_15_039.html> [10 December 2000].

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures.* Robert T. Marsh, Chairman (Washington, D.C.: GPO, October 1997). <http://www.info-sec.com/pccip/ pccip2/report_index.html> [28 December 2000].

Pufeng, Major General Wang. "The Challenge of Information Warfare." *China Military Science* (Spring 1995). In "Chinese Intelligence-Related Documents." *Federation of American Scientists.* <http://ftp.fas.org/irp/world/china/ docs/iw_mg_wang.htm> [8 January 2001].

Robertson, Lloyd. "Waging War On The World Wide Web." *CTV Television National News* (Pleasanton, CA: Community Television, 31 March 1999). Eden-Webster Passports/Lexis-Nexis [transcript online]. World News library. (7 January 2001)

Rodan, Gary. "The Internet and Political Control in Singapore." *Political Science Quarterly* 113 (Spring 1998). Columbia International Affairs Online [database online]. (9 January 2001)

Rothkopf, David J. "Cyberpolitik: The Changing Nature of Power in the Information Age." *Journal of International Affairs* 51 (Spring 1998). Columbia International Affairs Online [database online]. (9 January 2001)

Satchell, Michael. "Captain Dragan's Serbian Cybercorps (Serbs Used Internet For Propaganda, While NATO Drops Leaflets)." *U.S. News & World Report* 126 (10 May 1999). Eden-Webster Passports/Expanded Academic ASAP [database online]. #A54575536. (7 January 2001)

Shukman, David. *Tomorrow's War: The Threat of High-Technology Weapons* (New York: Harcourt Brace & Company, 1996).

Snow, Dr. Nancy. "The Smith-Mundt Act of 1948: A Fifty-year Legacy of U.S. Propaganda." *Peace Review* 10 (December 1998).

"Special: The Internet and the Law: Stop Signs on the Web." *The Economist* (11 January 2001). <http://www.economist.com> [15 January 2001].

Swett, Charles. Assistant for Strategic Assessment, Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. Policy Planning. "Strategic Assessment: The Internet." *Federation of American Scientists* (17 July 1995). <http://www.fas.org/cp/swett.html> [18 December 2000].

Thomas, Timothy L. "Kosovo and the Current Myth of Information Superiority." *Parameters* (Spring 2000). < http://carlisle-www.army.mil/usawc/Parameters/00spring/thomas.htm> [16 December 2000].

Thompson, Anne. "Spin Control: In Kosovo's Capital, the War Is All About Words with Yugoslavia." *The Associated Press* (8 August 1998). Eden-Webster Passports/Lexis-Nexis [database online]. World News library. (7 January 2001)

Timmes, Tom. Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict. Policy Planning. <timmest@mail.policy.osd.mil> "Re: PDD68." [E-mail to author <lungua@soc.mil>] June 9, 1999.

U.S. Defense Science Board. *The Creation and Dissemination of All Forms of Information in Support of Psychological Operations in Time of Military Conflict* (Washington, D.C.: GPO, May 2000).

U.S. Department of State. "About the Office of International Information Programs." <http://usinfo.state.gov/abtusia/aboutiip.htm> [5 January 2001].

U.S. Department of the Army. *Psychological Operations*, FM 3-05.30 (Washington, D.C.: GPO, 19 June 2000).

U.S. Joint Chiefs of Staff. *Joint Psychological Operations*. Joint Pub 3-53 (Washington, D.C.: GPO, 10 July 1996).

Weltz, Debra. Senior Doctrine Writer. PSYOP Division. U.S. Army John F. Kennedy Special Warfare Center and School. <weltzd@soc.mil> "RE: Law Reviews, Combined Smith-Mundt." [E-mail to author <angelamaria@lungu.com>] 14 December 2000.

"What is Public Diplomacy?" (20 June 1997). <http://www.publicdiplomacy.org/1.htm> [28 December 2000].

Yang, Dali L. "The Great Net of China." *Harvard International Review* (Winter 2001). Proquest [database online]. UMI. (10 January 2001)