AIR WAR COLLEGE

AIR UNIVERSITY

# PSYCHOLOGICAL OPERATIONS WITHIN THE CYBERSPACE DOMAIN

*by*

Prentiss O. Baker, LTC, USA

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

17 February 2010

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **17 FEB 2010** | | **00-00-2010 to 00-00-2010** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Psychological Operations Within the Cyberspace Domain** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air War College University,325 Chennault Circle,Maxwell AFB,AL,36112** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **Same as Report (SAR)** | **27** | |

## DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

# Contents

# *Illustrations*

*Page*

# Biography

LTC ( P) Prentiss Baker is an active duty Army Officer with 22 years of active service. He was commissioned as an Intelligence Officer where he served in a variety of positions at the Division Level and below. For the past 10 years, LTC Baker has been working at the Operational Level in his Functional Area, Information Operations, where he served as an Information Operations Planning Officer, Targeting Officer, and the Leader, Development and Education Chief for all newly assigned Army Information Operations Officers. He graduated in 1987 from Mississippi College with a B.S. in Mathematics and in 2003 from Touro University with a Masters of Business Administration. Following graduation from the Air War College, LTC (P) Baker will be assigned as the Chief, Information Operations for United States Army Central at Fort McPherson, Georgia.

***"WAR means fighting. But fighting is a trial of moral as well as physical forces, and the condition of the mind has always been the most decisive influence. ..." The physical factors "seem little more than the wooden hilt, while the moral factors are the precious metal, the real weapon, the finely-honed blade." Furthermore, if "moral forces" are the ultimate determinant of war, it then follows that the destruction of the enemy's will to resist should be the primary target in any conflict"……...Carl von Clausewitz***

**General.**

Wars embody political conflicts turned violent. They are fought to achieve political aims;[1] however, victory is rarely achieved through the destruction of an adversary's material. The key is to destroy the adversary's will to fight. Information Operations (Info Ops) is the primary means by which "will" and the ability to impose "will" and exercise command is attack.[2] An adversary's effectiveness is a function of his will and capability. Info Ops focuses on influencing the will and affecting those capabilities that directly enable the application of will.[3] To assist in achieving our political aims and the operational objectives of the Joint Force, we need a coherent integrated application of Information Operations across the range of military operations ( peace, war and stability operations) that encompasses all the domains (air, sea, land, space and cyberspace).

Psychological Operations (PSYOP), one of the core capabilities of Information Operations is critical to successful influence operations, and has been a vital part of warfare since ancient times.[4] PSYOP is defined by the U.S. military as, "planned operations to convey selected truthful information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of their governments, organizations,

[1] Clausewitz, *On War*, 69
[2] Joint Warfare Publication 3-80, *United Kingdom: Information Operations*, 12
[3] Ibid., 12
[4] JP 3-13, Information Operations, II-1

groups, and individuals."[5] Many great theorists and generals from Sun Tzu to Napoleon have emphasized the importance of waging Psychological Warfare.

***"One need not destroy ones enemy. One only needs to destroy his willingness to engage…"***
"***For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the supreme excellence."[6]*** ***Sun Tzu***

***"There are but two powers in the world the sword and the mind. In the long run the sword is always beaten by the mind…."*** ***Napolean Bonaparte***

There are numerous historical examples of armies and commanders effectively employing Psychological Operations in support of their campaigns and operations. From the reign of Alexander the Great in 300 BC to Operation Desert Storm/Shield and Operation Enduring/Iraqi Freedom, PSYOP was employed extensively to influence enemy forces to surrender, capitulate and/or abandon their equipment.[7]

Commanders and armies throughout history have been effective in employing PSYOP in the Land, Air, and Sea domains. Historical data documents the success of these commanders both on land, in the air and at sea using PSYOP; however, with the establishment of the cyberspace domain, this presents new opportunities and vulnerabilities for PSYOP forces operating in this domain. An understanding of the opportunities and challenges within this cyberspace domain is critical in developing a future operations concept for PYSOP forces, and employing PSYOP's mission essential functions effectively in future engagements.

Before Psychological Operations' mission essential functions can be effectively employed within the cyberspace domain, one must understand the dynamics, opportunities and the vulnerabilities this domain offers. There is no formal definition for the word "domain" within the military lexicon; however, it is generally understood within the military that a domain

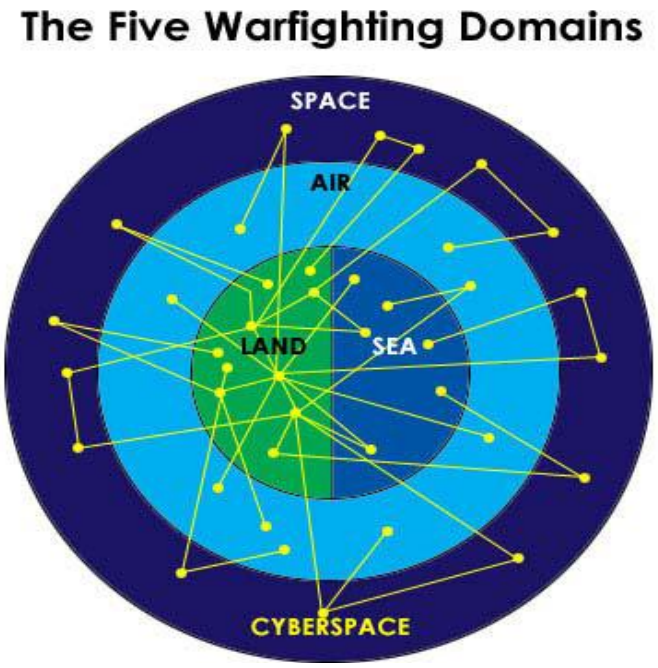
[5] JP 3-53, Psychological Operations, ix
[6] Tzu, The Art of War,
[7] Rouse, "History of PSYOP"

is a place where activities are performed to achieve some level of influence or control.[8] This assumes that there are other actors (hostile, neutral, or benign) who also operate in the domain and wield some influence—if only to protect their own ability to operate.[9] Joint Publication 1-02 defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[10] This domain presents some unique opportunities to influence, inform, and educate one's target audience. In this context the target audience is defined as "political and military decision makers, influential individuals, military personnel, armed factions, and specific population groups."[11]

Cyberspace as a domain (see figure 1) should be treated no differently than the traditional warfighting domains: that it, too, is an area of operations where success is defined by ones ability to orient, observe, decide and act faster than ones adversary.[12] In the book, *Combat Operations C3I: Fundamentals and Interactions,* George Orr describes a combat operations process that encapsulates the opportunities within all domains for the Joint Force Commander (JFC) to make better and faster decisions in order to apply the integrated employment of Info Ops capabilities at critical points within the cyberspace domain.[13]

[8] Elbaum, "Cyber Power in the 21st Century," 6
[9] Ibid., 6
[10] JP 1-02, Dictionary of Military and Associated Terms, 141
[11] Joint Warfare Publication 3-80, *United Kingdom: Information Operations*, 12
[12] Orr, *Combat Operations C3I*, 25
[13] Ibid., 25

**Figure 1 - Cyberspace exists across and affects objects in the other four domains**[14]




The JFC's ability to understand and manage the sources of potential power (i.e the capabilities of Information Operations and more specifically Psychological Operations) is key in exploiting opportunities as they arise within the cyberspace domain.

In short, cyberspace will become, if it has not already, the center of gravity for our nation and many others. Further, it is a contested operating environment in which people and organizations are attempting to control, deny, or restrict our ability to use and exploit —in other words, cyberspace is a domain, just like air, land and sea.[15] Given this, it is imperative that a JFC understand the opportunities that this domain offers, and where applicable applies all available military means to include PSYOP effectively to achieve the operational objectives.

[14] Elbaum, "Cyber Power in 21st Century," 6
[15] Ibid., 7

## Purpose.

The purpose of this *Future Operating Concept (FOC)* is to describe how future Joint Force Commanders can employ Psychological Operations' mission essential functions in the cyberspace domain to assist in accomplishing his/her operational objectives in the 2015-2020 timeframe. This FOC will guide the development and integration of Joint Force Commander's PSYOP concepts and capabilities for an integrated employment of PSYOP capabilities within the cyberspace domain.

In addition this FOC will also provide a basis for further PSYOP/Cyber discussion, debate, and experimentation intended to influence subsequent PSYOP/Cyber concept and capability development. It will also influence Joint and Service combat development processes by helping the joint force gain a better appreciation of the challenges and opportunities that will result in conducting PSYOP in the cyberspace domain.

Finally, this concept contributes to further development of a comprehensive FOC that encompasses all the elements of Information Operations, (Electronic Warfare, Operation Security, Military Deception, and Computer Network Operations) in an integrated concept that feed Joint and Service transformation plans. The overall desired end state is a joint force with an enhanced capability for conducting PSYOP within the cyberspace domain integrated with the other core and supporting capabilities of Info Ops that allows the joint force to create operational effects in the cyberspace domain as effectively as it does in the land, air and sea domains.

## Time Horizon, Assumptions and Risks.

This FOC covers the time horizon from 2015 – 2020. In the development of this FOC an assumption was only considered if it meets the following criteria: 1) It should be a likely future

condition, but not a certainty; 2) Its future validity is necessary for the concept to be valid. [16]The following are key assumptions of the FOC:

- In 2015-2020, the United States will face conflicts involving state and non-state actors that will use the cyberspace domain to confront the United States and its strategic partners.
- The Department of Defense will have funding and authorities to support and employ persuasive and cyber technologies within the cyber domain.
- The joint force will be required to conduct operations in the cyber domain and cyber operations projects in support of other operational objectives.
- The cyber domain will become the domain of choice for our adversaries to take advantage of persuasive and cyber technologies to influence individuals to support their cause and to create an atmosphere of fear.
- Cyber Command will protect the Global Information System and will provide the necessary capabilities to exploit and attack systems within cyberspace.

## Description of the Military Problem.

The complexity of the future security environment is rooted in global and regional ideological and political struggles. These struggles will challenge traditional US military approaches. "Faced with the conventional warfighting capacity of the United States, our adversaries will likely choose to fight using a hybrid of irregular and asymmetric capabilities as a way to achieve their objectives."[17] They will seek to undermine and erode the national power, influence, and will of the United States and its strategic partners while vigorously using the cyberspace domain to recruit, influence and solidify its ideological base.

[16] Joint Operating Concept, "Irregular Warfare,"13
[17] Ibid., 16

The future operational environment includes a mix of military and non-military challenges by state and non-state actors to a Joint Force, with irregular and asymmetric warfare as the favored form of warfare of those who would be our adversaries including near peer competitors.[18] Many of the actors that we will encounter in this environment are technologically savvy and fully understand the opportunities that exist in the cyber domain to recruit, influence, threaten, and manipulate emotions. The cyber domain in turn provides an operating environment, protection, and cover for our adversaries. The competition for the uncommitted populations within the cyber domain will be one of the key PSYOP objectives of the Joint Force Commander.[19]

This pervasive operating environment within the cyberspace domain will present the Joint Force Commander with several operational problems. How can JFCs effectively employ PSYOP capabilities in the cyber domain to take advantage of the opportunities that this domain presents while mitigating the vulnerabilities within the domain in order to gain or maintain control or influence over a relevant population? The Joint Force must determine how to:

- Conduct cyber operations to influence adversaries, relevant populations and states through Information Operations means.
- As a supported effort, counter our adversary ability to use the cyber domain to influence, recruit and intimidate relevant population.

**Factors That Compound the Joint Force Problem.** Conducting PSYOP within the cyber domain will present the following challenges for the future joint force:

- The expanding scale of Cyber Operations, and the threat of cyber influence, attacks and exploitation will become increasingly global in scale beyond the traditional area of operation.

[18] Joint Operating Concept, "Irregular Warfare," 17
[19] Ibid., 18

- The unbounded scope of the cyberspace domain will disadvantage the joint force. Our adversaries will be unlikely to operate under the same legal or moral restrictions as will the joint force.
- The expansion of the cyber-operational area to non-belligerent states. Adversaries are likely to operate within and from non-belligerent states that crosses several Combatant Commands' area of responsibilities which will restrict joint force authorities.

**Synopsis of the Central Idea:**

Given that war remains a pre-dominantly a human endeavor, the cognitive dimension is central to this concept. In a set of contiguous and noncontiguous operations using the cyberspace domain as a joint operations area, the JFC must employ PSYOP across all three dimensions (physical, informational and cognitive) of the information environment necessary to influence our adversaries or relevant publics, in order to convince the target audiences to accede to our will or modify their behavior.[20]

At this point, a model would be helpful to conceptualize the kind of activities which would be effective in achieving the desired result (influence target behavior, protect friendly behavior from being influenced). All PSYOP activities occur within the broader context of an information environment. This environment recognizes the critical role that information and information systems play in today's advanced societies as they progressed along a continuum from agrarian, to industrial, to the information age.[21] This environment pervades and transcends the boundaries of land, sea, air, space, and cyberspace. It is accessible and leveraged by both state and non-state actors. Within this environment exist three conceptual dimensions: physical,

[20] Department of Strategy, *Information Operations Primer AY09*, 17
[21] Ibid., 18

information, and cognitive, representing a target's decision cycle.[22] The physical dimension includes the systems/computers, the information dimension represents the data that is stored on these systems, and the cognitive dimension focuses on the mind of the decision maker or users of the data/systems.[23] PSYOP actions across these dimensions are enabled by the fluid and integrated employment of all Info Ops capabilities across the cyberspace domain, leveraging persuasive and cyber technologies in a networked environment to increase precision delivery of message, unity of purpose and coherency in action. The integrated application of Info Ops within the cyberspace domain can be a major force multiplier and set the conditions for the JFC's operational success in the other warfighting domains.

**Application and Integration of PSYOP functions within Cyberspace Domain.**

With the emergence of the cyberspace domain and the opportunities which exists within this domain, the potential for PSYOP to exploit and take advantage of this domain is astronomical. In "*Cyber Silhouettes: Shadow over Information Operations"* the author, Mr. Timothy Thomas concludes, "there is a collapse of big media, society as a whole is relying more on virtual products rather than newspaper and other forms of print."[24] This assertion has been validated from statistical data analyzed over the past ten years. The data substantiates that there has been an exponential rise in the use of the cyberspace domain. As of September 2009, there were 1.74 billion internet users growing at a rate of 380% from 2000-2009. [25] A fourth of the world's population is now connected to the internet.[26] The number of mobile cellular subscribers worldwide will reach the 4 billion mark by the end of 2009 which accounts for over half of the

[22] Department of Strategy, Information Operations Primer AY09, 17
[23] Joint Publication 3-13, *Information Operations,* I-2
[24] Thomas, Cyber Silhouettes, 278
[25] Miniwatts Marketing Group, "Internet World Stats"
[26] Ibid.,

world population. [27] "The number of subscribers has surged nearly 25 per cent annually for the past eight years. Mobile penetration stood at only 12 per cent in 2000, growing to reach over 60 per cent by the end of 2008." [28] If these trends continue, one can assume that at least three fourths of the world will be operating within the cyberspace domain by 2020.

Given this rise in the use of virtual products and the cyber domain by society, it is imperative that our PSYOP Forces understand and take advantage of this domain to influence our adversary leadership, military personnel, relevant populations and other non-state actors to modify their behavior in a manner that is favorable to the JFC objectives. In order to take advantage of the opportunities that the cyber domain offers, one must be adept in the employment of the vast array of persuasive/cyber technologies. PSYOP forces must be prepared and equipped to take advantage of the opportunities while reducing the vulnerabilities that the cyber domain offers in support of the Joint Force Commander.

Persuasive technologies are critical in influencing and modifying individuals' behavior. There are numerous types of cyber technology that can be used to persuade people: internet, web sites, mobile phones, PDAs, interactive video games, virtual reality, desktop software, chat bots, and social network sites.[29] It is imperative that our PSYOP professionals take advantage of these cyber technologies along with this target rich "cyber' environment to influence relevant populaces. Our adversaries are already taking advantage of these persuasive and cyber technologies to influence individuals to support their cause and to create an atmosphere of fear.[30] Several terrorists' organizations are using, blogs, cell phones, websites and email to recruit individuals and to provide direction and command and control of activities.

[27] Miniwatts Marketing Group, "Internet World Stats"
[28] Bilello, "Cell Phones Subscribers to Hit 4 Billion this Year"
[29] Fogg, Persuasive Technology, 5
[30] Thomas, Cyber Silhouettes, 279

The cyber domain and persuasive technologies offers several advantages in the area of influence. First, cyber and persuasive technologies are interactive allowing one to tailor program as situation evolves and based upon target audience input.[31] Secondly, in the cyber domain these persuasive technologies can be more persistent than humans. Machines can work around the clock to persuade an individual.[32] Third, these cyber and persuasive technologies can offer greater anonymity. This allows the target to overcome social forces and culture that lock people routines making them more susceptible to the influence techniques.[33] Fourth, the information being presented to influence can be easily modified and changed in the cyber domain to address the target audience.[34] Lastly and perhaps the most important is that these persuasive technologies through the cyber domain allow access. These cyber and persuasive technologies can go where humans cannot go or may not be welcome. [35] The opportunities and potential access to an enormous target audience through the cyberspace domain enhances our PSYOP forces' ability to influence critical audiences in support of the JFC.

In support of the Joint Force, PSYOP Forces have been directed to perform several mission essential functions (See Appendix 1). Operational PSYOP are conducted across the range of military operations, including during peacetime, in a defined operational area. [36] Critical to this Future Operating Concept is the ability of the JFC's PSYOP forces to effectively execute these mission essential tasks within the cyberspace domain.

To take advantage of the opportunities that the cyberspace domain offers, Col ( R ) John Boyd's Observe, Orient, Decide and Act (OODA) concept provides some insights on how the

[31] Fogg, Persuasive Technology, 7
[32] Ibid., 7
[33] Ibid., 8
[34] Ibid., 8
[35] Ibid., 8
[36] Joint Publication 3-53, *Psychological Operations,*

JFC might be able to make faster decisions and re-distribute power within the cyberspace domain.[37] Boyd's OODA concept aim is to diminish adversary's capacity while improving our capacity to adapt as an organic whole, so that our adversary cannot cope while we can cope with events/efforts as they unfold.[38] From a PSYOP perspective the focus is on the "orientation" part of the concept in order to "penetrate adversary's moral-mental-physical being to dissolve his moral fiber, disorient his mental images, disrupt his operations, and overload his system, as well as subvert, seize those moral-mental-physical bastions, connections, or activities that he depends upon, in order to destroy internal harmony, produce paralysis and collapse adversary's will to resist."[39]

For the JFC to take advantage of these opportunities, PSYOP forces must understand the relationship between the information environment and cyberspace domain. The information environment, as discussed previously consists of three dimensions (physical, informational, cognitive) in which our adversaries and relevant audiences will operate. Cyberspace is a man-made domain that interconnects and networks all three dimensions of the information environment. The multi-verse (metaverse) which is a key component of the cyberspace domain resides across each of these dimensions. The multi-verse (metaverse) is defined as, "the convergence of virtually enhanced physical reality and physically persistent virtual space. It is a fusion of both, while allowing users to experience it as either."[40] This multi-verse (metaverse) is divided into four distinct cyber-operating environments, virtual worlds, and mirror worlds, life-logging and augmented realities all of which provides unique opportunities to influence, inform,

[37] Osinga, "A Discourse on Winning," 25
[38] Ibid., 25
[39] Ibid., 26
[40] Smart, *Metaverse Roadmap,* 4

or educate a specific target audience maneuvering in these spaces. [41] Within the 2015 - 2025 timeframe, these multi-verses connected by cyberspace will become more technologically advance and more widely used.

Virtual world is a computer based simulated environments.[42] Within the virtual world, for example, PSYOP forces will be required to conduct virtual to virtual engagements with target audiences to influence in support of the JFC objectives. These virtual to virtual engagements will augment and in some cases replace the face to face engagements that PSYOP forces are required to do in the physical domains. PSYOP forces will also be required to established radio and television programming within these virtual worlds to disseminate JFC's messages in order to inform, educate and influence. In addition, these virtual worlds will also provide popular venues to emplace posters, bulletin boards and community letters that will reach a wide target audience. The opportunities within the virtual world for PSYOP forces to produce and disseminate messages to specific target audiences are limitless.

Mirror worlds are informationally-enhanced virtual models or "reflections" of the physical world. Their construction involves sophisticated virtual mapping, modeling, and annotation tools, geospatial and other sensors, and location-aware and other lifelogging (history recording) technologies.[43] These mirror worlds will also provide PSYOP forces will unique opportunities to perform mission essential functions within cyberspace domain. These mirror worlds can be extremely useful in assisting PSYOP forces in performing target audience analysis prior to producing and disseminating messages. Mirror worlds will provide key insights to gathering sites, favorite media outlets, and other information conduits that can be utilized in support of their missions.

[41] Smart, *Metaverse Roadmap*, 5
[42] Ibid., 5
[43] Ibid., 9

Life-logging is the capture, storage and distribution of everyday experiences and information for objects and people. This practice can serve as a way of providing useful historical or current status information, sharing unusual moments with others, for art and self expression, and increasingly, as a kind of "backup memory," guaranteeing that what a person sees and hears will remain available for later examination, as desired.[44] Imagine the opportunities that this information will provide PSYOP forces if they are able to access and manipulate this information in support of PSYOP missions. This information will allow PSYOP forces to develop very precise target audience analysis, and tailor messages and programs for a specific group or individual using one's own life experiences as the foundation to influence or modify a behavior.

The interconnectivity of cyberspace also provides opportunities to influence groups of people by leveraging social influence.[45] Because of their networking capability, mobile technology and networked computing products brings groups of dispersed people together. As the recent protests in Iran (2009) show, people can generally achieve a greater degree of attitude and behavior change working or acting together as a cohesive group.[46] PSYOP forces can use the principle of social facilitation through cyberspace domain to influence groups of people at the same time. Social facilitation concludes that, "people are more likely to perform a well-learned behavior if they know they are being observed via computing technology, or if they can discern via networked technology that others are performing the desired behavior along with them."[47] The cyberspace domain provides the PSYOP professionals the opportunities to leverage the

[44] Smart, *Metaverse Roadmap*, 14
[45] Fogg, *Persuasive Technology*, 196
[46] Ibid., 197
[47] Ibid., 197

principle of social facilitation to influence groups of individuals to change or modify their behaviors.

PSYOP forces can also create situations within cyberspace domain that leverage normative influence to change people's behavior or attitudes. Normative influence works through a process that exploits peer pressure, or what psychologists refer to as pressures to conform.[48] People tend to change or modify behaviors to match the expectations, attitudes, and behaviors of the team, family, tribe, clan or other groups commonly referred to as the "in-group".[49] PSYOP forces can track or create representations of individuals exhibiting the desired behavior within the "in-group" and using the multi-verse to share this information with others in the group/family/tribe/clan to pressure them to conform.

In addition to leveraging peer pressure, PSYOP forces can utilize the cyberspace domain to undermine peer pressure by encouraging and influencing people to resist the pressure to conform. People are more capable of resisting group conformity influence when at least one person defies the group.[50] Within cyberspace or the multi-verse, this one person can be created in the virtual world and leverage against individuals or groups in the real world. An example of this is: Suppose groups of youths are being pressured and recruited to join terrorist groups via virtual worlds and social network sites. PSYOP using technology within the cyber domain could convincingly portray individuals within the "in-group" that have successfully resisted recruitment efforts. This could be a powerful use of PSYOP within cyberspace to counter terrorist recruitment.

The use of PSYOP within cyberspace to affect the decision-making calculus of select individuals in a regime who represent the hub of decision-making power is critical. To influence

[48] Fogg, *Persuasive Technology*, 199
[49] Ibid., 199
[50] Ibid, 200

within the cognitive dimension, PSYOP can rely on a strategy of personal contact established via cyberspace to influence and persuade. Private contact with the target audience is an important element in this dimension. It directly influences the target audience sense of vulnerability yet allows the selected target audience the opportunity to save face and not be seen as capitulating to overt diplomatic or military pressure. The inducement of ―private pressure can be employed quite creatively within the cyberspace domain to produce a psychological effect that results in modification of behavior or policy.[51]

The emergence of the cyberspace domain has created significant opportunities for PSYOP forces to perform mission essential functions in support of the JFC. By utilizing the emergence of virtual worlds, mirror worlds and life-logging within the "multi-verse", PSYOP can gain critical access to wider audiences leveraging the phenomenal of social influence/facilitation to influence their target audience while providing the target with a level of anonymity that doesn't exist in the physical world.

**Necessary Capabilities.**

To effectively execute PSYOP mission essential functions within the cyberspace domain, new computing capabilities and persuasive technologies will be required. When it comes to influencing attitudes and behaviors, timing and context are critical. Intervening at the right time and place via networked, mobile technology increases the chance of achieving the desired effects.[52] Some of the capabilities that will be required for PSYOP to be effective in the cyberspace domain are listed in Appendix 2.

[51] Bohannon, "Cyberspace and the new Age of Influence," 79
[52] Fogg, *Persuasive Technology*, 183

**Challenges:**

The PSYOP approval process is excruciatingly slow and has been often characterized as being unresponsive to the need of the commander. Operating within the cyberspace domain can significantly reduce these shortcomings; however, this can potentially open the door to other problems. PSYOP products are required to be pre-tested with the potential target audience; however, working in cyberspace may not be conducive to adequately pre-testing products which could lead to unintended effects. This lack of quality control and pre-testing of PSYOP products can create problems because once the products have entered the cyber domain and are circulating within the multi-verse (metaverse), it is almost impossible to recall the product. These products are also extremely vulnerable to manipulation from adversaries if not monitored closely.

In addition to the slow approval process, another significant challenge is the command and control of PSYOP/Cyber forces within the JFC. The asymmetric nature of cyberspace and the far reaching implications of disseminating PSYOP's products across the cyberspace domain increase the possibility of information fratricide. The JFC's PSYOP programs that are executed within the cyberspace domain have the potential to cross several other Functional Commands and Combatant Commands areas of responsibilities. This potential requires a clear command relationship (Tactical Control, Operational Control, Administrative Control) between the affected commands to ensure battlespace de-confliction.

The last challenge is the legal and ethical concerns with conducting PSYOP within the cyberspace domain. U.S. law prohibits PSYOPing the American populace. Within the physical warfighting domains (land, sea, air), PSYOP messages, broadcasts, leaflets and handbills can be disseminated to the desired foreign target audiences with little to no implications on the American public; however, within the cyberspace domain this becomes extremely difficult and

will require additional measures to ensure the American populace exposure to PSYOP products are minimized. With respect to PSYOPing foreign audiences especially children, this will present the JFC with ethical challenges that are not associated with the other domains. Children and other very vulnerable audiences are susceptible to PSYOP techniques that were not available in the other domains. If these techniques are exposed by our adversary this could become a public relation nightmare.

**Summary.**

It is this perpetual extension of influence through cyberspace that Thomas Friedman describes when he recounts how the advent of the modem-equipped personal computer ―gave individuals in this flattening world both reach and scale—reach because they could create content in so many new and different ways and scale because they could share their content with so many more people.[53] This age, like others before it, has entered into a bold new era of warfare marked by innovative technologies that are changing the face of conflict. Whether the development of the microchip, the invention and global distribution of the Internet, and the creation of a cyberspace domain have brought about a revolution in military affairs or are part of a larger evolution of military practice has not yet been determined. What is certain, however, is that cyberspace has presented itself as a new and undeniably significant domain in which to conduct military operations. This concept demands a theory for how PSYOP forces ought to be employed in this new realm.[54]

[53] Friedman, *The World is Flat*, 58
[54] Bohannon, "Cyberspace and the new Age of Influence," 77

## BIBLIOGRAPHY


Atkinson, S.R.(2009). Cyber: *Envisaging New Frontiers of Possibility*. Defence Academy of the United Kingdom Occasional paper.

Atkinson, S.R. and A. Goodman (2008). Influencing Network Decision Taking. CCRP, ICCRTS Conference, 9 and draft ARAG Occasional paper.

Air Force Doctrine Document 2-5, 11 January 2005. *Information Operations.*

Bilello, Suzanne, "Number of cell phone subscribers to hit 4 billion this year, UN says," 2008, http://portal.unesco.org/ci/en/ev.phpURL_ID=27530&URL_DO=DO_TOPIC&URL_SECTION=201.html, accessed 18 Nov 2009.

Bohannon, Leland MAJ USAF. "Cyberspace and the New Age of Influence." School of Advance Air and Space Studies. Maxwell AFB, Alabama: Air University, June 2008.

Defense, Department of. *Joint Vision 2020*. Washington DC: Government Printing Office, 2000.

Department of Strategy, Operations and Planning and Center for Strategic Studies, *The Information Operations Primer 2008*. U.S. Army War College, Carlisle Barracks, PA, 2009.

Elbaum, Joseph M. MAJ USAF. "Cyber Power In The 21st Century." Air Force Institute of Technology. Wright-Paterson AFB, Ohio: Air University, December 2008

Fogg, B. J. Persuasive Technology: Using Computers to Change what we Think and Do. San Francisco, CA: Morgan Kaufman Publishing, 2003.

Friedman,Thomas L., The World Is Flat : A Brief History of the Twenty-First Century, 1st Picador ed. (New York: Picador/Farrar Straus and Giroux : Distributed by Holtzbrinck Publishers, 2007.

Joint Publication 1-02, 19 August 2009. *Department of Defense Dictionary of Military and Associated Terms*

Joint Publication 3-13, 13 February 2006. *Information Operations*

Joint Publication 3-53, 5 September 2003. *Doctrine for Joint Psychological Operations*

Joint Warfare Publication 3-80, June 2002. *United Kingdom: Information Operations*

Joint Operating Concept (JOC) Version 1.0, 11 September 2007. *Irregular Warfare (IW)*

Joint Operating Concept (JOC) Version 1.0, September 2004. *Major Combat Operations (MCO)*

Joint Operating Concept (JOC) Version 1.0, 11 September 2007. *Stability Operation (SO)*

Lungu, Angela M. MAJ, USA. "WAR.COM: The Internet and Psychological Operations."

Naval War College. Newport, RI: Department of Joint Operations, 2001.

Miniwatts Marketing Group, "Internet World Stats," 2009 http://www.internetworldstats.com/stats.htm, accessed 18 Nov 2009

Orr, George E. *Combat Operations C3I: Fundamentals & Interactions.* Maxwell Air Force Base: Air University Press, 1983.

Osinga, Frans COL. "A Discourse on Winning and Losing: Introducing Core Ideas and Themes on Boyd's Theory of Intellectual Evolution and Growth." Quantico, Virginia, 13 July 2007.

Rouse, Ed. MAJ. "History of Psychological Operations." http://www.psywarrior.com/psyhist.html, accessed 25 October 2009

Schmitt, John F. *A Practical Guide for Developing and Writing Military Concepts*. DART: Working Paper #02-4, 2002.

Smart, John E., Jamais Cascio, and Jerry Paffendorf. *Metaverse Roadmap: Pathways to the 3D Web*, A Cross-Industry Public Foresight Project, San Pedro, California: Acceleration Studies Foundation, 2007.

Thomas, Timothy L. *Cyber Silhouettes: Shadows Over Information Operations.* Foreign Military Studies Office, Fort Leavenworth, KS, 2005.

Tzu, Sun. *The Art of War*. Basic Books. New York, NY. 10 Feb 1994

Wentz, Larry. Barry, Charles L. Starr, Stuart H., *Military Perspectives on Cyberpower.* The Center For Technology and National Security Policy at The National Defense University Washington, DC July 2009.

Wray, Richard. "Half world's population 'will have mobile phone by end of year," Sep 2008, http://www.guardian.co.uk/technology/2008/sep/26/mobilephones.unitednations. accessed 18 Nov. 2009

Universal Joint Task List, Joint Staff, Washington, D.C. 15 January 2009.

## Appendix 1 PSYOP Mission Essential Functions

Listed below are the PSYOP mission essential functions as outlined in Joint Publication 3-53 and the Universal Joint Task List.

- **Inducing or reinforcing** foreign attitudes and behavior favorable to the JFCs objectives.
- **Developing, designing, producing, distributing, disseminating, and evaluating** PSYOP products and actions to achieve the overall campaign objectives.
- **Promoting** the effectiveness of the joint force commander's (JFC's) campaigns and strategies
- **Strengthening** US and multinational capabilities to conduct military operations in the operational area Support military-to-military programs as part of Theater Security Cooperation agreements.
- **Advising** the supported commander through the targeting process regarding targeting restrictions, psychological actions, and psychological enabling actions to be executed by the military force.
- **Influencing** foreign populations by expressing information through selected conduits to influence attitudes and behavior and to obtain compliance or noninterference with friendly military operations.
- **Providing** public information to foreign populations to support humanitarian activities, ease suffering, and restore or maintain civil order.
- **Serving** as the supported commander's voice to foreign populations by conveying the JFC's intent.
- **Countering** adversary propaganda, misinformation, disinformation, and opposing information to correctly portray friendly intent and actions, while denying others the ability to polarize public opinion and affect the political will of the United States and its multinational partners within an operational area.
- **Attack** adversary legitimacy and credibility
- **Build and sustain** support among selected foreign TAs
- **Shift** loyalty of adversary forces
- **Promote** the cessation of hostilities.
- **Undermine** adversary confidence
- **Persuade** isolated and bypassed adversary forces to surrender
- **Educate** the selected foreign TAs in liberated or occupied territory

## Appendix 2 Additional Capabilities

This list is not all inclusive and will require additional discussion and debate from both Cyber and PSYOP professionals to fully identify all necessary capabilities.

- The JFC will need to be able to access relevant foreign populace mobile technologies, the data that reside on networks and authorities to manipulate data.
- Authority and capability to established web sites in support of the JFC.
- Ability to exploit and disrupt web sites within the JOA that is enticing undesired behaviors.
- Cyber professionals trained in the art of influence. PSYOP forces knowledgeable in operating within the cyberspace domain.
- Tools to monitor internet usage and popular social network sites within the JOA.
- Capability to establish JFC PSYOP operated radio/TV broadcasts via the internet.
- Authority and capability to produce and disseminate PSYOP products via cyberspace.
- Ability to collect and monitor information within cyberspace.
- Ability to measure the effectiveness of PSYOP operations within cyberspace.
- The ability integrate Info Operations capabilities within cyberspace and across the other domains.
- The ability to plan and execute nested and coherent Information Operations across all domains.
- The necessary authorities to conduct PSYOP using cyberspace at the JTF.
- Revision of PSYOP doctrine to include the use of cyberspace domain as medium for dissemination.
- Regional cultural experts to monitor and to engage foreign audiences via cyberspace.
- Human Terrain Teams that are experts in Human Factor Analysis and cyber operations.
- Unified Command Plan that expands the responsibilities for PSYOP to other services.