

IO SPHERE

September 2012

The Professional Journal of Joint Information Operations

Information Operations Intelligence Integration

IN THIS ISSUE

- IO Intelligence Integration
Maj Gen Shanahan pg2
- Joint IO Assessment Part II
Mr. Charles Chenoweth pg4
- Culture Has Consequences
Dr. Gary Buffington pg8
- Intelligence: Key to Success in IE
Mr. Joshua Cook pg10
- Militant Radical Islamic Website: IJU IO
Ms. Karen Kaya pg12
- Tactical MISO for Low Intensity Conflict
LTC J.R. Reiling pg17
- Evolution of IOII
Mr. Joshua Cook pg22
- Tendency Analysis
Mr. Mark Conder pg27
- Cultures and Organizations:
How IOII Supports Non-Lethal Operations
CPT Gustavo Molina pg29
- Face and IO
Maj Douglas Wilber pg32



Joint Information Operations Warfare Center





FEATURE ITEMS and ARTICLES



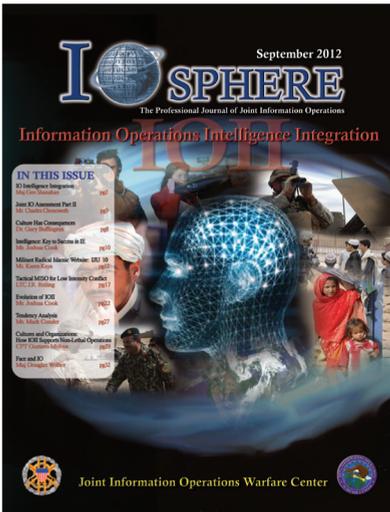
Information Operations Intelligence Integration (IOII)	
John N.T. Shanahan, Major General US Air Force	2
Joint Information Operations Assessment Methodology: Part II	
Mr. Charles Chenoweth	4
Culture Has Consequences	
Dr. Gary Buffington	8
Intelligence Community: The Key to Success in the Information Environment	
Mr. Joshua Cook	10
The Anatomy of a Militant Radical Islamic Website: The IJU's Information Operations	
Ms. Karen Kaya	12
Structuring Tactical Military Information Support Operations for Low Intensity Conflict	
LTC J.R. Reiling, US Army	17
Evolution of Information Operations Intelligence Integration	
Mr. Joshua Cook	22
IO Sphere Transition to the Digital Age	26
Tendency Analysis	
Mr. Mark Conder	27
Cultures and Organizations: How IOII Can Support Successful Non-Lethal Operations	
CPT Gustavo A. Molina, US Army	29
Face and Information Operations	
MAJ Douglas Wilber, US Army Retired	32

Credit and thanks to our graphics and layout editors Ms. Gloria Vasquez, Ms. Sharon Singleton, Ms. Jill Winters, and Mr. John Reyna of the US Air Force ISR Agency, and copy editor Mr. Bruce Judisch, MeriTec Services Inc. and the JIOWC.

Printed by the Air Force Intelligence, Surveillance & Reconnaissance Agency Print Plant, San Antonio, Texas, Mr. Rosalio Martinez, Director and Mr. Abiodun Quadri, Printing Services Director.

About the Covers: The front and back cover represent the various aspects of Information Operations Intelligence Integration.

About our Cover Design: The IO Sphere cover is symbolic of the importance of Information Operations in the global projection of national power. The base layer is a map of the world. The cover colors are a representation of the US military service colors and the color purple to symbolize the joint nature of Information Operations.



Cut Along Line

IO Sphere Key Staff

Maj Gen John N.T. Shanahan
 Dep Dir for Global Operations, Joint Staff J-39
CAPT Samuel D. Schick
 JIOWC, Director
Ms. Laura Hawkins
 JIOWC J-5, Executive Editor
Mr. Bruce Judisch, MeriTec Inc, Copy Editor

Mr. Henry (Keith) Howerton
 Editor and Layout Design
 Webhead Inc
Mr. Myron Hustoft
 Digital Editor and E-Reader Layout
 MeriTec Inc
LTC Krisada Shaw and Mr. Ed Ratcliffe
 Executive Editors and Editorial Board Directors



If you're on a .mil network, then *IO Sphere* is available to you on the Joint Staff's JDEIS electronic publishing site.

Go to <https://jdeis.js.mil/jdeis/index.jsp>, and look at the left-hand listing at the bottom, then click on Additional Resources and JIOWC IO Sphere.

IO Sphere can also be found on SIPRNet at:

<http://intelshare.intelink.sgov.gov/sites/jiowc/publications/default.aspx>

Endnote references for all **academic** articles are published with the article. Contact the Editor for questions about endnotes.

Note: From .mil official domains CAC credentials are required.



Afghanistan Visit

**Undersecretary of Defense for Intelligence,
Mr. Michael Vickers, visits Coalition Forces
in Afghanistan**



GENERAL SUBMISSION GUIDELINES:

IO Sphere welcomes submissions of articles regarding full-spectrum IO, including all information-related capabilities and activities. *IO Sphere* also welcomes book reviews and editorial commentary on IO and defense-related topics. Submission deadlines do not guarantee placement in next issue. So, it is best to send a submission when it is ready as it may take several issues to include accepted submissions. The *IO Sphere* staff will decide status of all submissions and work to get it included in a future issue.

TEXT - Microsoft Word.

CHARTS/GRAPHS - TIFF, GIF, JPG format or Microsoft PowerPoint with maximum of one full size chart or graph on each slide.

PHOTOGRAPHS - TIFF, GIF or JPG in 200 dpi resolution or higher. Please place graphs/photographs/charts on separate pages or as file attachments.

FORMAT/LENGTH - 500 words or more double spaced.

**Send letters to the editor,
articles, press releases &
editorials to:**

jiowc.iosphere@us.af.mil
Or

Joint Information Operations
Warfare Center - IO Sphere
2 Hall Blvd., Suite 217
San Antonio, TX 78243-7074
Phone: (210) 977-5227 DSN: 969
FAX: (210) 977-4654 DSN: 969

CALL FOR ARTICLES

IO Sphere is currently seeking submissions on all information-related activities including military information support operations, IO training and education, IO support to public diplomacy, public affairs, communication strategy, electronic warfare, IO intelligence integration, and IO assessments.

Disclaimer Statement

This Department of Defense publication (ISSN 1939-2370) is an authorized publication for the members of the Department of Defense and interested stakeholders. Contents of the *IO Sphere* are not necessarily the official views of, or endorsed by, the US Government, the Department of Defense, the Joint Staff, or the Joint Information Operations Warfare Center. The content is edited, reviewed for security, prepared, and provided by the J-55 Advocacy Office of the Joint Information Operations Warfare Center under the direction of the US DOD Joint Staff J-39/Deputy Director for Global Operations (DDGO). Authors are required to conduct security review of all submissions with their own organization. All photographs are the property of the DOD or JIOWC, unless otherwise indicated. Send articles, Letters to the Editor, or byline editorials to jiowc.iosphere@us.af.mil or Joint Information Operations Warfare Center, Attn: *IO Sphere* Editor, 2 Hall Blvd, Ste 217, San Antonio, Texas 78243-7074. **Articles in this publication may be reproduced without permission. If reproduced, *IO Sphere* and contributing authors request a courtesy line and appropriate source citation.**

Views from the Top

Information Operations Intelligence Integration (IOII)

By

Maj Gen John N.T. Shanahan
Deputy Director for Global Operations
Joint Staff J-39

I don't blame you if you admit that you are not familiar with the abbreviation, IOII. Neither was I, at least until fairly recently. Yet the term Information Operations Intelligence Integration is an exceptionally important one. It captures the very essence of how IO and intelligence must be fused in a way that enhances the best of both disciplines. Indeed, we cannot have it any other way in today's global environment. As someone who has commanded an Intelligence Group, a command and control wing, and an ISR flying wing, and who now owns IO and Military Information Support Operations (MISO) as part of the Joint Staff J-39 portfolio, I am – and will always be – one of the joint community's most ardent advocates for improving the integration of IO and intelligence.

We live in a world that is increasingly complex, with a fascinating juxtaposition of non-state chaos in some areas and near-peer nation state competitors in others. Information is the new coin of the realm. Yet information in isolation is



useless. Or, even worse, bad or inaccurate information can drive actions that are counter-productive and even destructive. Information only becomes useful and actionable when fused by high-quality intelligence. This is true from the tactical to the grand strategic level, from unclassified open sources through compartmented special technical operations, and from carbon-based HUMINT to space-based SIGINT and everything else in between. There is a rapidly growing need for strong collaboration between intelligence and operations to counter an increasingly nebulous global threat environment, one in which the term "potential adversary" can lose its qualifier overnight. Such ambiguity creates a unique problem set. Countering it demands the tightest possible integration of intelligence activities with operational planning and execution during every phase of operations, from peacetime Phase 0 operations through crisis and full-blown combat operations, to enabling civil authorities after conflict ends. Nowhere is this truer than in the IO arena, an arena that includes as much art as science and that, because of its complexity and reputation as a 'fuzzy' discipline, leads some to conclude – most erroneously – that successfully integrating IO and intelligence is a fool's errand.

So what is IOII? Quite simply, it is the integration of multi-source intelligence information into the planning, execution, and assessment of information-related capabilities (IRC). It resides at the very heart of any information operation. Quality intelligence is fundamental to the precise application of IRCs, and equally vital to the assessment of the application of the same. IOII professionals supporting the integration of IRCs are among the best the intelligence community has to offer, but they face daunting challenges. A significant capability gap lies between the vast amount of information sources and the limited number of intelligence resources available to exploit them. Similarly, the extremely fine granularity of intelligence needed to effectively employ IRCs presents the intelligence collector and analyst with the proverbial needle-and-haystack conundrum in gleaning the most accurate information from the best sources. Collectors and analysts themselves often lack unique state-of-the-art skills, knowledge and abilities to provide accurate, relevant, and timely intelligence support to planners and operators. These factors create a formidable, but not insurmountable, barrier to intelligence elements supporting IO integration initiatives.

The IOII community of action (COA) is meeting these challenges head on, developing analytic tradecraft, establishing training standards, developing doctrine, and identifying available resources across the Defense Intelligence Enterprise. Their collaborative efforts address a wide range of topics, including force development, targeting, and intelligence support to IO assessment. Constrained by shrinking budgets, bridging IOII capability gaps requires conceiving, refining, and implementing processes and procedures across the DOTMLPF spectrum with an eye toward adopting or adapting non-material

Global Information Operations Collaboration

Located on All Partners Access Network (APAN), this site provides access to an electronic *IO Sphere* library, IO doctrine and policy library, document repositories, forums for sharing information or asking questions, Wiki library, and chat functions. Includes sub-groups for best practices, IO training and force development, and IO requirements and advocacy.

<https://communities.apan.org/ioc>

**Virtual Collaboration for the IO Community Including
Allied Partners**



solutions before seeking to develop new materiel ones. A lot has been done – but we still have a long way to go.

This issue of *IO Sphere* highlights the various aspects of IOII and the initiatives the COA is undertaking. The articles set the stage and provide the background and context to fully understand and appreciate IOII, while detailing specific efforts underway to address the remaining challenges. IOII must not be an isolated discipline, exclusive to a single COA. If IO is to attain its true potential as a force multiplier and become an integral tool in the commander's tool kit, it requires the interaction and involvement of the entire Department, the interagency, and private/commercial non-governmental entities. I welcome your suggestions on how we can get there.



John N.T. Shanahan
Major General, USAF



Maj Gen John N.T. "Jack" Shanahan is the Deputy Director for Global Operations, Operations Directorate, Joint Staff, the Pentagon, Washington DC. He is responsible to the Chairman of the Joint Chiefs of Staff for oversight and coordination of worldwide operational matters. This includes reconnaissance, information operations, space and missile defense, military information support operations, and special technical operations. He has served in a variety of flying, staff and command assignments including Branch Chief in the Operations Directorate at Headquarters US Pacific Command, and senior military assistant to the Assistant Secretary of Defense for International Security Affairs. He has commanded the USAF Weapons School Support Division, 480th Intelligence Group, 505th Command and Control Wing, and 55th Wing.

IO SPHERE IS GOING DIGITAL

San Antonio, TX-(August 6, 2012) Since the first issue in spring of 2005, *IO Sphere* has become the premier journal for the profession of military information operations (IO). Over the years, thousands of print copies have been distributed all over the world to operational, academic, intelligence and other interested organizations and readers. However, as with so many other worthwhile endeavors, the *IO Sphere* is feeling the impact of current fiscal constraints and changes in readership preferences.

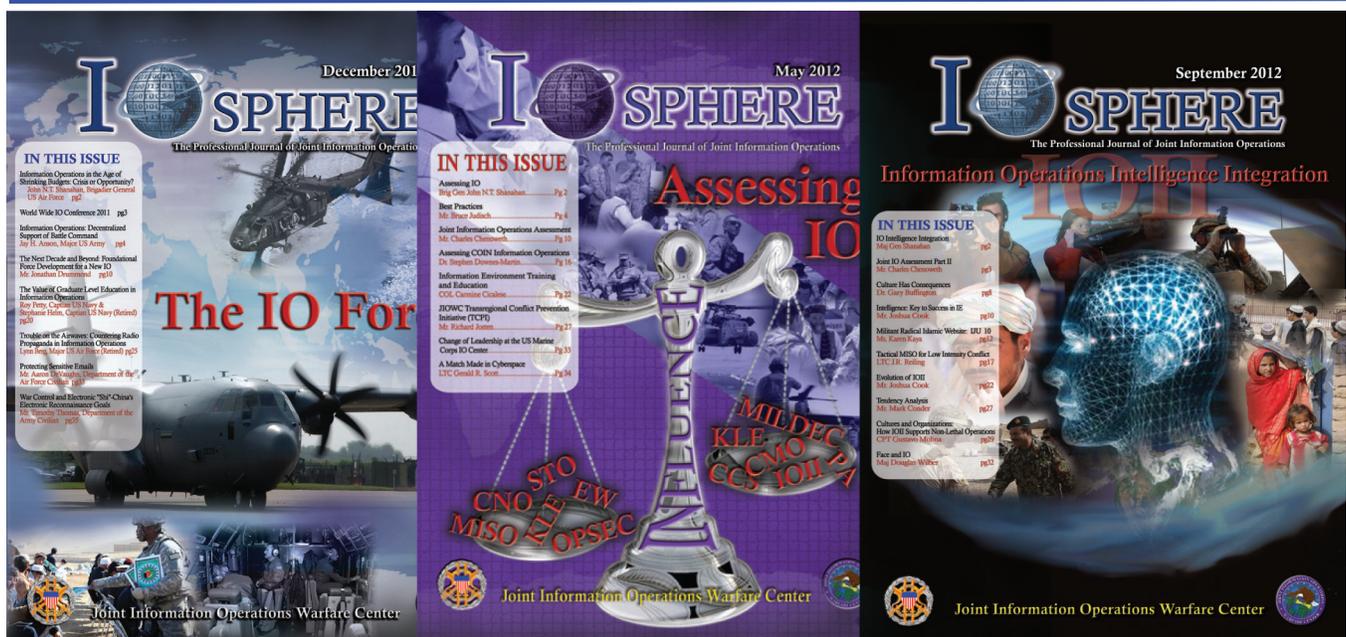
Not only is printing and distribution of hard copies often expensive, the demand for a print copy is simply not as strong as it once was as more and more readers are turning to digital devices as a reading mode of choice. Therefore, beginning in the fall of 2012, the *IO Sphere* will no longer appear in the traditional print version, but rather in a digital format.

Although this is, for the most part, a positive move, it comes with some challenges being addressed by the *IO Sphere* staff to keep the readership engaged and interested in being

a part of *IO Sphere*. The *IO Sphere* staff and leadership are researching ways to deliver the digital version using the best possible authorized digital publishing solutions; for example, on compact disk, in Web-based format, e-magazine style, and through applications for smart phones and tablet devices. It will likely take us a couple of issues to get all this sorted out, so we request your patience. At a minimum, though, *IO Sphere* will continue to appear in Adobe PDF format and posted on the Joint Doctrine Education and Training Electronic Information System (JDEIS) and the All Partners Access Network (APAN) Global Information Operations Collaboration page, as well as, other IO organizations and academic web sites.

IO Sphere is the most relevant scholarly journal and informative periodical for the joint and allied IO community. That will not change as this new digital era of the journal is embraced.

Suggestions from readership as we transition to an all-digital version are welcomed. Please address any questions or comments to the editor at jiowc.iosphere@us.af.mil.



Joint Information Operations Assessment Methodology-Part II

By

Mr. Charles Chenoweth

Editor's Note: Assessment of the effectiveness of all military lines of operation is essential. Policy makers, senior leaders, and budget makers need good analysis and feedback to justify expenditures. In IO, this process can be very difficult. Mr. Chenoweth's essay is a primer on how the community to assess IO more effectively. This is part two of a two-part series of articles on this subject.

My first article on assessment, published in the May 2012 issue of *IO Sphere*, was titled Joint Information Operations Assessment Methodology. It discussed the reasons for the increased focus on assessment, JIOWC's new task to develop a joint IO assessment framework, and the general concept of the IO assessment methodology that focused primarily on steps 0 through 3 of the eight-step joint IO assessment process. It also gave some examples of models and discussed possible procedures to help derive assessment information from complex problems.

In this article, I will cover the remainder of the steps, (4-7) and provide more information on models. When the staff completes steps 0 through 3 (remember, it looks linear, but is iterative in nature), the commander is ready to execute the planned activities. In Step 4, execute IO and ISR activities, the staff uses the collection plan developed during step 2 to coordinate execution with collection requirements. For time-sensitive IO activities, there may need to be close coordination between ISR providers and the operational executors, as the activities may require immediate monitoring of indicators to develop valid assessment data.

Other planned activities may not require such immediate observation. During execution, planned activities need coordinated monitoring; therefore, the task definition within the plan should not only describe the task, but also the collection requirements, so that the IO executor understands his/her assessment reporting responsibilities. Some questions to answer when writing the tasks include the following: What are the procedures of IO execution? Is it the type of activity that will require immediate collection of measures of performance (MOP) in order to record and capture the execution for assessment? Will a situation report be required in order to validate that the task was conducted and what was specifically done? Will a synchronization matrix help align IO activity execution with MOP and measures of effectiveness (MOE) monitoring-particularly for events that require time-sensitive targeting? Is there a non-traditional actor conducting the task, and how will this actor report completion and effectiveness of the task? By providing assessment-reporting criteria for the IO executor in the tasking order, the assessment staff can be notified when IO activities have occurred and then alter the plan based on potential or actual changes in the information environment (IE). Doing this will help alleviate one of the main problems we face, which is the lack of assessment criteria in every phase of the planning process.

Step 5, monitor and collect data for IO assessment, is the continuous process of observing progress toward task accomplishment and objective achievement. During this step, germane assessment data is collected, aggregated and consolidated. Gaps in the assessment data are identified and

Step 0	Characterize the information environment (IE)
Step 1	Integrate IO assessment into plans
Step 2	Develop IO assessment information requirements and collection plans
Step 3	Build IO assessment baseline
Step 4	Execute IO and ISR activities
Step 5	Monitor and collect data for IO assessment
Step 6	Analyze IO assessment data
Step 7	Report IO assessment results and recommendations

Figure 1 - Joint IO Assessment Methodology

highlighted in order to determine actions to be accomplished to alleviate shortfalls. Assessment results and recommendations help commanders adjust operations and resources, assist in determining when to execute branches and sequels, and assist in making other critical decisions to ensure current and future operations remain aligned with the mission end state, which leads us to Step 6.

During Step 6, the staff compares the assessment data to the baseline to identify (1) changes in the IE, and (2) whether the IO activities had their desired effect. This is an iterative process that contains feedback loops to the relevant groups involved in the process. The information environment analytic construct (IEAC), is a repeatable analytic construct that provides a way to measure the effects of IO-related activities. The construct, as presented in figure 2, enables an analyst to characterize how an action within the IE creates a measurable indicator that can be compared to the baseline.

Information-related activities are categorized as changing conditions associated with either a will or a capability. These activities then become mechanisms to alter the environment to achieve desired effects. If there are no changes in the IE, the analysis process may include reviewing the analytic or logic model to identify flaws in logic.

As we continue to improve IO assessment, one of the keys will be in learning how to create robust models of the IE. Ideally, these will be models that provide an ability to simulate and visualize how the system operates and interacts with other systems.

The IEAC is a descriptive model that develops an abstraction

of the real world that defines motivational stimulus for a target audience. This model is an excellent first step in developing an ability to simulate and visualize how complex human systems operate. Shaping the IE involves attempting to modify a complex human system. These complex human systems are open systems; that is, they relate, exchange, and communicate with other systems. Open systems cannot be defined or analyzed through a reductionist scientific process; therefore, better IO assessment will involve developing more robust models of systems that accurately portray the environment and better simulate how the system interacts with other systems. A robust model that describes the system as a whole will help create a better predictive model for course of action development. A better predictive model, in turn, can support and identify more detailed effects which will cascade throughout the planning and assessment process to provide better assessments and ultimately better operations.

In Step 7, report assessment results and recommendations, the staff develops actionable recommendations to address the findings and prepares the summary report. The assessment report ultimately will provide recommendations for plan adjustment, analysis of return on investment, a new IO assessment baseline, and a synopsis on overall mission success towards achieving the desired end state. Both formal and informal communication channels need to be developed among the participants in this process. When relevant new information is obtained, whether within planning, execution, collection or analysis, it needs to be relayed to appropriate personnel when they most need it, not just during Step 7. The IO assessment report will ultimately provide feedback to IO planners and

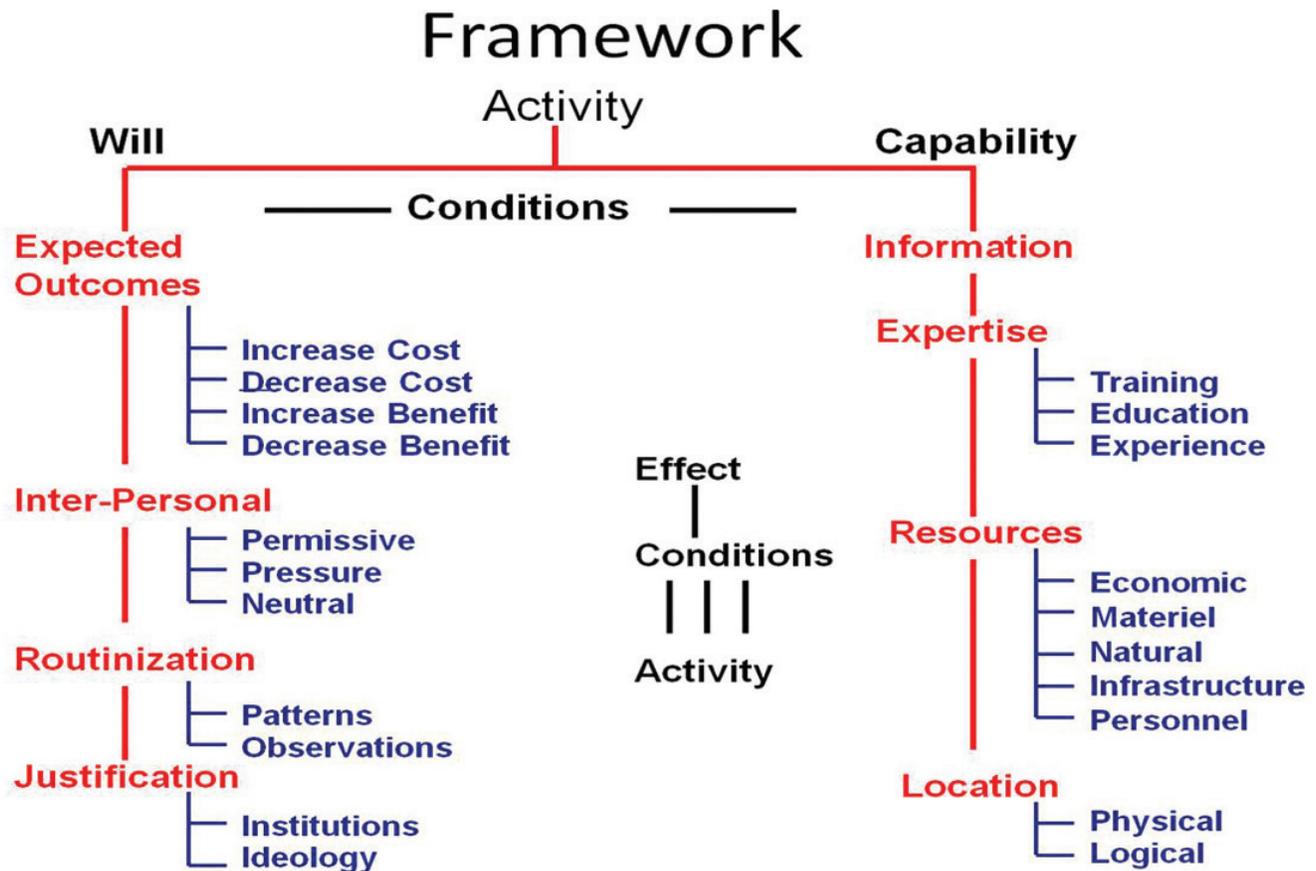


Figure 2 - Analytic Construct for Joint IO Assessment

operational commanders, and at the same time, the operational evaluation of the effectiveness of activities conducted will provide data that can feed programmatic analysis and policy. On the programmatic side, IO operational assessment can feed data to the Joint Staff, the Office of the Secretary of Defense, and Congress. This assessment information can provide situational awareness to governance regarding IO actions and expenditures and support determination for funding of critical IO activities. Additionally IO operational assessments can identify the degree to which IO actions, along with the concomitant effects and consequences, support higher-level guidance found within strategic documents such as the National Security Strategy and Guidance for Employment of the Force.

The IO assessment framework will continue to evolve as the IO community comes under greater pressure to justify resources for information-related activities and the acquisition of greater information-related capabilities. In the past, it was acceptable simply to highlight what was done without regard to the effectiveness of those activities. For future operations and activities, assessment is going to be a large part of the equation. The IO assessment framework is a model to use for that process, and it gives commanders and other programmatic decision-makers important information on the effectiveness of IO activities.



Mr. Charles Chenoweth is a retired US Navy Commander and surface warfare officer. He currently serves as a Department of The Air Force civilian as the J31 Assessments Branch Programs coordinator at the JIOWC in San Antonio, Texas. He has extensive background in all aspects of Information Operations including planning and assessment of IO and the effectiveness of information related activities.



MAKE A DIFFERENCE JOIN THE FA 30 TEAM



*Become a
US Army IO Officer*



The US Army Information Proponent Office wants active-duty officers to join Information Operations. IO is the Army's fastest growing functional area. IO officers assist commanders to understand, visualize, describe, direct, assess and lead the Army on today's information battlefield. IO officers have opportunities for:

- **Competitive Promotion**
- **Advanced Civil Schooling**
- **Training with Industry**
- **CONTACT: HRC FA 30 Career Management Officer (502-613-6130), IPO Personnel Chief (913-684-9432), or e-mail: usarmy.leavenworth.tradoc.mbx.usaipo-pa-planner@mail.mil**

CHECK OUT THE IPO WEBSITE

<http://usacac.army.mil/cac2/IPO/>

JOINT INFORMATION OPERATIONS PLANNERS COURSE



Joint Forces Staff College

Only DOD Certification Course for Joint IO Planners

DOD Requirement for Joint IO Planning Billets

Earn College Credits



MISO
CNO
MILDEC
EW
OPSEC



Public Affairs
Defense Support to
Public Diplomacy
CMO

Physical Attack
IA
Physical Security
CI
Combat Camera

Visit our Website
www.jfsc.ndu.edu

Learn About

IO Related Capabilities
Intelligence Support to IO
Joint Operational Planning Process
Interagency Coordination
IO Integration and Synchronization
Emerging Concepts and IO
Planning Tools

Graduates Will

Understand the Complexity and
Construct of the Information
Environment
Know Joint IO Theory and Doctrine
and the Effects of IO
Become Proficient in the Joint
Operational Planning Process
Be Prepared to Serve as a Lead
IO Planner in a Joint IO or IO-
Related Planning Position

Sponsored by the Joint Command, Control, and Information Operations School,
Joint Forces Staff College

Apply online at http://www.jfsc.ndu.edu/schools_programs/jc2ios/io/default.asp
or contact the registrar at (757) 443-6337/ DSN 646-6337

Culture Has Consequences

By

Dr. Gary W. Buffington

Editor's Note: Dr. Gary Buffington's views on culture are important, and understanding the cultural dynamic in the context of Information Operations Intelligence Integration is a critical link in quality analysis. Dr. Buffington is a valued and learned academic in his field of study. *IO Sphere* is very pleased to provide the platform for sharing his views.

Culture has consequences, and those consequences can be deadly.

The almost successful assassination of Tooryalai Wesa, Afghanistan's provincial governor of Kandahar, on Saturday, 28 April 2012, proves the point. Two insurgent gunmen shot their way to the threshold of Wesa's office before being killed by security guards because they leveraged Afghan cultural sensitivities to their advantage.

What became a 20-minute firefight began with the two insurgents smuggling small pistols into the governor's compound hidden inside their shoes under the soles of their feet. Contributing to the attackers' initial success—two guards were killed in the initial moments of the attack—was their knowledge that the guards would not ask them to remove their shoes at the security checkpoint. As the provincial police chief, Brig-Gen Abdul Raziq, explained to reporters afterwards, "We can't take the shoes off people who are coming to visit the governor, nor take off their turbans and let them visit the governor, bare feet and heads. This is a violation of our culture, and the enemies want to distance the government from civilians by using such tactics."

The role of culture in both intelligence analysis and in the formulation of an effective information operations (IO) campaign plan cannot be understated. The study of culture becomes the vehicle that searches out the themes and ordering propositions of a people or a target audience. In so doing, the study of culture seeks to answer such questions as: "How

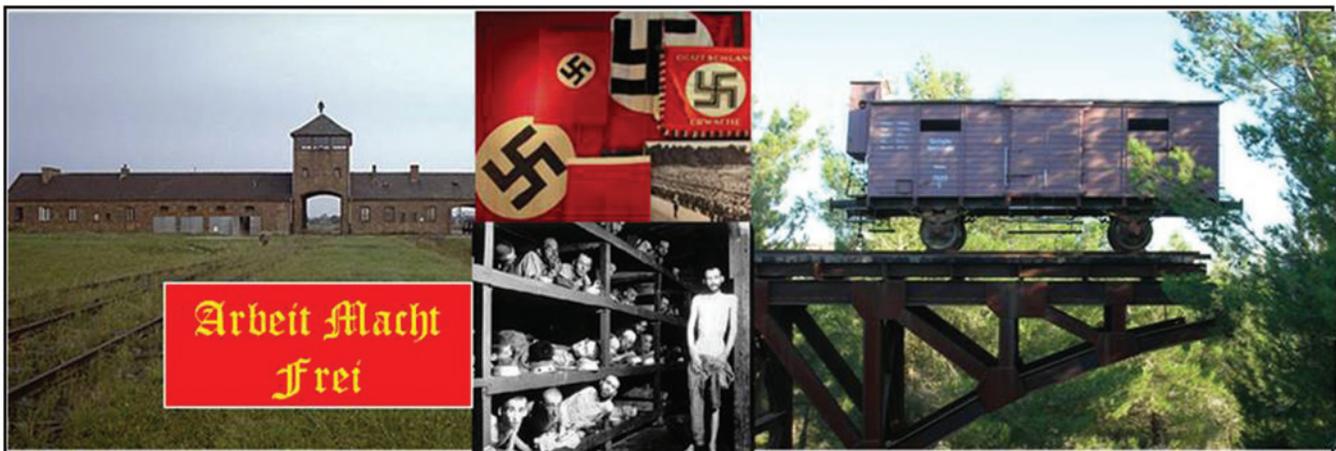
do people portray their lives?" "What do they imagine life to be about?" "How do people represent pain, reward and aspirations?"

However, the study and understanding of culture is not as simple as one may think. The American anthropologist, Dr. Clifford Geertz (1926—2006), summarized the challenge facing analysts and research specialists. "Everyone knows what cultural anthropology is about: it's about culture," he said. "The problem is that no one is quite sure what culture is."

Dr. Geertz defined culture as "historically transmitted patterns of meanings embodied in symbols" by which people "communicate, perpetuate and develop their knowledge about and attitudes toward life." In this context, culture becomes an "acted document," a "set of stories," and a "collective text" handed down from generation to generation. The telling of these stories, Dr. Geertz contends, which is done both in actions and words, "consists of what people say and do, and in [the] doing, [what they] 'say' about themselves."

In this construct, therefore, culture can be seen as a "text" that can be "read." And if culture is a "text" that can be "read" it can also be "interpreted" much as a literary critic interprets literature. Thus a person's life becomes the subjective experience of the collective cultural "text" that one lives. By interpreting this "text," the analyst discerns aspects of that person's self and his surrounding society. By such interpretation and discernment, the IO practitioner can craft themes and messages that resonate within that cultural text.

Comprehending the nuances of a foreign culture is not an easy task, for the outside analyst is confronted with a complex web of information, all of which guides a target audience's actions, experiences and perceptions with varying degrees of interaction. Because culture forms the sum total of the learned behavior of either an individual or a select group of people, it should be considered their traditions and their way of life. As such, a people's symbols, heroes and rituals—the visible, tangible aspects of a culture—and their values—the invisible,



To understand the modern-day nation state of Israel and to comprehend the collective psyche of the Israeli people, one must "read and interpret" the impact of Nazi Germany's "Final Solution" on the Jewish populations of Europe.

intangible aspects of a culture—are accepted generally without conscious thought as they are passed along from one generation to the next.

Among the common or shared characteristics of diverse cultures is that it is learned. The “rules of a culture” are taught by members of the community, usually from the older to the younger. Cultures contain patterns based on repetitive actions or activities that give understanding to individual purpose and behavior. Cultures consist of shared behaviors or beliefs held in common by groups within the greater community. Finally, cultures are cumulative with “new” inventions or advances evolving from previous developments in incremental stages.

Failure to comprehend these nuances of culture can yield results that range from the humorous to the disastrous. The story is told about the failure of General Motors to market their very popular US brand, Chevy Nova, in South America. The “suits” in the GM front office could not understand why their Latin American sales of this highly successful brand were so abysmal. It was not until someone pointed out to them that no Spanish-speaking driver would ever purchase a car that “No va” that GM finally changed their marketing strategy.

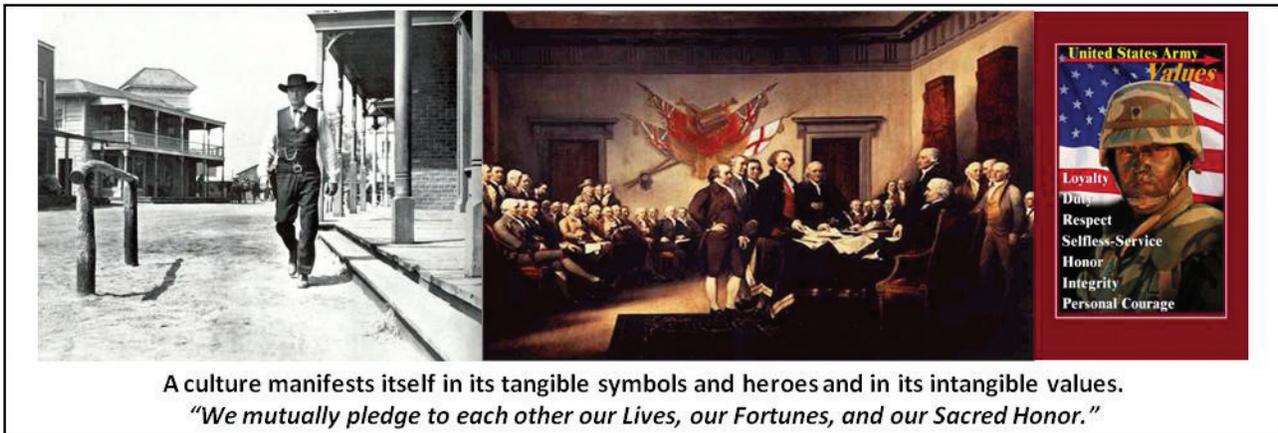
Far more tragically were the cultural mistakes that led to the Indian Mutiny of 1857—referred to also as the “Sepoy Rebellion.” While this revolt had many contributing causes, the spark that ignited the revolt was the decision by the British East India Company to issue the Pattern 1853 Enfield Rifle to their native regiments. The Enfield used a paper cartridge that was dipped in tallow to make it waterproof. This led to rumors being spread among the Hindu regiments that these cartridges were covered in grease derived from cows. Similar rumors spread among the Muslim regiments claimed that the Enfield cartridges were coated in hog fat. Since the loading procedure required the rifleman to bite off the end of the cartridge, this

procedure would be culturally abhorrent to both Hindu and Muslim levies. Tragically, British efforts to defuse these rumors served only to reinforce their “truth” in the minds of the Sepoys. In the resulting two-year rebellion, at least 11,000 British soldiers were killed and untold thousands of Sepoys and civilians also perished.

As these two examples indicate, culture consists of the thoughts, beliefs, practices and behaviors of either an individual or a group of people. These cultural markers embrace history and religion and dictate how a society organizes itself socially, politically and economically. Their influence extends even to the production of goods and services. Culture not only influences people and their actions at national, regional and local levels, it impacts relationships across gender, generational and social class boundaries. Understanding these cultural interchanges is essential for the IO practitioner to craft an effective influence campaign.



Dr. Gary W. Buffington is a retired US Air Force Chaplain. He holds a doctorate degree in Ministry and has extensively traveled the world. He has authored several studies on the role of religion and cultural research, as well as many works on the ideological foundations of Islamic extremism and other totalitarian movements. At the time this article was written he worked as a Human Factors Senior Analyst at the Joint Information Operations Warfare Center in San Antonio, Texas.



IO Education and Training Catalog of Courses

Located on All Partners Access Network (APAN), the Joint Staff J-39 and J-7 (JCW) have sponsored the listing of IO training opportunities available to the IO community. View the catalog at:
<https://community.apan.org/ioc/iofd-t/p/tng.aspx>

Please Submit Questions or Updated Information on the Catalog to
Mr. Michael Broster, 210-977-4701 (DSN 969)
or email michael.broster.1@us.af.mil



Intelligence Community: The Key to Success in the Information Environment

By
Mr. Joshua Cook

Editor's Note: Mr. Josh Cook is a staunch advocate of ensuring the intelligence community properly supports the IO fight. His hard work in organizing the IOII effort into a movement, then groups, and eventually into a community of action has been incredibly important to effectively employing information-related activities. His contribution to *IO Sphere* is very welcome.

The Director of National Intelligence Vision 2015 called on the Intelligence Community (IC) to “integrate the Community through mission-focused operations that transcend agency and functional silos. We confront the challenge of acting in an environment that is more time sensitive and open to the flow of information, in which intelligence sources and analysis compete in a public context established by a global media.”¹ Combining that direction with: “We see globalization—growing interconnectedness reflected in the expanded flows of information, technology, capital goods, services and people throughout the world—as an overarching ‘megatrend,’ a force so ubiquitous that it will substantially shape all the other major trends in the world of 2020,”² and the fact that the information environment (IE) is the common denominator of the key drivers and trends for 2020 as identified by the DNI’s Vision 2015, we are left with the need to examine how the IC is poised to analyze the IE.

The IE is defined as “the aggregate of individuals, organizations, and systems that collect, process disseminate, or act on information.”³ Key audience beliefs, perceptions, and reactions are crucial to the success of any given strategy, policy, plan, operation, or activity to maintain decision superiority in the face of today’s key drivers and trends. They must therefore be identified, understood, and when appropriate, actively addressed. Individual actions and words may seem benign in the near term, but often have a temporal and cumulative effect

“...the key to intelligence-driven victories may not be the collection of objective ‘truth’ so much as the gaining of an information edge or competitive advantage over an adversary. Such an advantage can dissolve a decision-maker’s quandary and allow him to act. This ability to lubricate choice is the real objective of intelligence.”

*Jennifer Sims, Director of Intelligence Studies,
Georgetown University*

on key audiences that can yield strategic effects. How does the vision of communicating strategically translate into the intelligence community prioritizing, analyzing, and providing the requisite intelligence in the face of the challenges outlined in the DNI Vision 2015, the National Intelligence, and these new realities that: 1) all forms of national power depend on information; 2) information and technology are vital to national security; and 3) our adversaries fully maximize information’s value?

Information Operations (IO) is defined as “the integrated employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.”⁴ The new definition focuses on integration of capabilities, something not lost on the IC.

In 2009, the Intelligence Support to Information Operations (ISIO) Community of Interest (COI) changed its name to reflect the integrating nature of our work, as well as demonstrate our



Factors of Globalization

intent to proactively engage the issues facing the collective. We became the Information Operations Intelligence Integration (IOII) Community of Action (COA) and defined IOII as “the integration of intelligence disciplines and analytic methods to characterize and forecast, identify vulnerabilities, determine effects, and assess the IE (physical, information, and cognitive dimensions).” The integration of intelligence disciplines (human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, open-source intelligence, technical intelligence, and counterintelligence) is critical to characterize and forecast, identify vulnerabilities in, determine effects of, and assess the IE. However, the real meat on the bone is the analytic methods such as socio-cultural analysis (SCA) and human-terrain mapping (HTM) that play a key role for IOII.

SCA informs the understanding of people by analyzing societies, populations, and other groups of people. This includes their activities, relationships, and perspectives across time and space at varying scales. SCA is employed in many mission-specific intelligence frameworks (e.g., human factors, human-terrain analysis and mapping, operational environment analysis, regional and national stability analysis, weapons proliferation analysis). SCA draws upon the social sciences and the humanities; e.g., anthropology, area studies, cultural studies, demographics, history, human geography, political science, social psychology, and sociology. It contributes to all-source and multi-INT analysis for the full spectrum of military operations and for a wide range of interest to policymakers. Analytical concepts distinctive to SCA include, but are not limited to, social structure, norms, socio-cultural identity, beliefs, values, ideologies, narratives, common knowledge, and proximity.

HTM integrates geo-referenced social, cultural, political, economic, infrastructure data, and elements of the IE into all-source and multi-INT analyses relating to areas of operation. It is a mission-specific, tailored form of intelligence analysis. HTM can provide analytical insights into the activities, relationships, and perspectives of groups of people in relation to operations. Whereas SCA and HTM are considered the “meat on the bone,” cyberspace intelligence could be considered the skeletal foundation for IOII. The explosive growth in the use of information technologies—the Internet, social networking, cell phones, news media, etc.—within the cyberspace domain is reshaping and changing the IE at unprecedented rates. This constantly changing landscape is causing both subtle and not-so-subtle changes to the SCA and HTM baselines, increasing the complexity of the IE; an example is the cyberspace domain’s amorphous nature. The full impact of the physical, information, and cognitive aspects of the cyberspace domain on IO and IOII is still being explored.

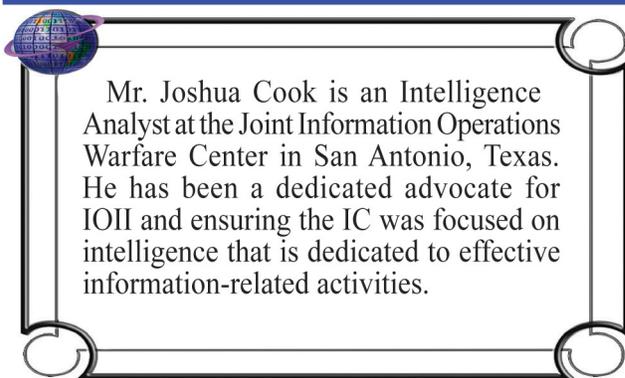
As you can see, many communities—e.g., IO, IOII, SCA, HTM, and cyberspace—are attempting to understand key audiences

and their influencing factors to create the information-decision advantage over our adversaries. Put simply, these communities are all in the IE intelligence integration business, regardless of whether it’s from the physical, information, or cognitive dimensions. The real question is “Are legacy intelligence prioritization frameworks adequately structured to provide the intelligence vitally needed to understand and operate in the IE?” And the unsurprising answer is: “No, they are not.”

One of the most complex yet compelling issues facing us is the demand for change in how the defense intelligence enterprise is organized and orchestrated to respond to the demands of our operational partners. Understanding and shaping the IE are critical to successful operations. Yet, our ability to build that understanding and determine the shape of the IE is constantly under siege, due in large measure to the current intelligence prioritization schema within which we operate. Neither the National Intelligence Priorities Framework nor the Defense Intelligence Priorities Framework clearly delineates the need for intelligence that supports the understanding and shaping of the IE. We, as the IC, have expressed this concern through a number of studies and reports over the last three years. In addition, while there are pockets of awareness throughout the IC at senior levels, we need to turn the tide on an outdated structure to answer key intelligence questions asked by the national leadership to ensure intelligence-driven victories in the future. While the need may be simply stated, the actions needed to effect change are not so simple. The IOII COA will focus on developing those actions and seeking support from our community and our operational partners to close the intelligence gaps in our ability to characterize, understand, and shape the IE. ●

Endnotes:

1. *Director of National Intelligence’s Vision 2015.*
2. *National Intelligence Council, “Mapping the Global Future, 2020.”*
3. *Joint Publication 1-02, “Department of Defense Dictionary of Military and Associated Terms.”*
4. *SECDEF Memorandum on SC & IO in the DOD 25 January 2011*



Mr. Joshua Cook is an Intelligence Analyst at the Joint Information Operations Warfare Center in San Antonio, Texas. He has been a dedicated advocate for IOII and ensuring the IC was focused on intelligence that is dedicated to effective information-related activities.



The Anatomy of a Militant Radical Islamic Website: The Islamic Jihad Union's Information Operations

By
Ms. Karen Kaya

Article Synopsis and Editor's Note: This article analyzes the information operations and public relations strategy of the Islamic Jihad Union (IJU), a coalition of Islamic militants from Uzbekistan and other Central Asian states, who are closely related to Al-Qaida. The analysis is based on thorough monitoring and examination of statements, videos and updates that the group posts to its Turkish-language website. It explores their target audience and their themes and messages with a view to identify how the group recruits, gain supports and perpetuates its militant radical Islamic ideologies through comprehensive public relations campaigns. The article also aims to provide insight into the IJU's future motivations. Since analysis of radical websites is an important part of IOII about radical Islamic threats, this article is a important contribution to this issue of *IO Sphere*.

Introduction

The Islamic Jihad Union (IJU) is a coalition of Islamic militants from Uzbekistan and other Central Asian states closely related to Al-Qaida and the Taliban (Figure 1). The group conducts a comprehensive information operations campaign on its Turkish language website sehadetzamani.com ("time for martyrdom"), where it uses an ideologically powerful recruitment appeal to attract militants, gain support, and perpetuate its ideology (Figure 2). Close monitoring and examination of statements, videos and updates that the group posts to the site reveal the group's strategy, its target audience and its themes and messages; while revealing its goals, targets and future motivations.

The IJU is believed to have evolved from the Islamic Movement of Uzbekistan (IMU), an Uzbek-dominated terrorist group linked to Al-Qaida. The group was an obscure organization before it surfaced in 2004, when it claimed responsibility for bombings in the Uzbek cities of Tashkent and Bukhara which killed 47 people in March and April 2004. The group's largest attacks or attempted attacks were the July 2004 bombing of the US and Israeli embassies in Tashkent, Uzbekistan, and its September 2007 foiled plot to bomb the US Air Force base in Ramstein, Germany, along with the US and Uzbek consulates in Germany. Their statements claiming responsibility for the attacks are an important part of their information operations.

Although the IJU started out with a goal of establishing an Islamic state in Uzbekistan, in recent years, it has expanded its objective to establishing an Islamic caliphate in Central Asia. It calls for Muslim unity, attracting Pakistani, ethnic Turkish, Chechen, Arab, and other recruits outside the immediate Central Asian region. The group has also been referred to as a



Figure 1. Islamic Jihad Union Banner
Source: sehadetzamani.com



Figure 2. Islamic Jihad Union Website
Source: sehadetzamani.com

"Turkish Al-Qaida," for two reasons: first, the IJU's website, sehadetzamani.com, is in Turkish and promotes militant 'jihadi' ideologies and its affiliation with Al-Qaida; second, despite its Uzbek background, the content of the group's website has a strong Turkish element in its international support and recruitment networks. Based on information on its website, the group is currently active in Afghanistan and cooperates with the Taliban, conducting small-scale operations against US and NATO forces.

The IJU's Information Operations

It is unclear when the group adopted sehadetzamani.com as its mouthpiece (Figure 2). The website advocates militant jihad through its articles, and hosts an array of violent videos from militant radical Islamic media organizations affiliated with Iraq and Afghanistan. Some of the videos also make their way into YouTube, the popular video-sharing site. The site's colorful, technically-advanced home page is obviously a militant radical Islamic page, indicating that the group is targeting those who already espouse such ideologies; not trying to persuade or convert anyone into joining the "jihad."²

The IJU produces a wide range of sophisticated public relations materials, including a series of statements about the group's small-scale actions in Afghanistan. It features videos showing the organization's training camp, members preparing for suicide attacks, and farewell interviews with suicide bombers. Significantly, most of this content is published or recorded in Turkish. The group has even produced its own Turkish hymn, which it uses as the opening song for their videos (with the repeating refrain "We are the mujahedeen of the Islamic Jihad Union").

Themes and Messages

The group's comprehensive information operations strategy includes carefully thought-out themes and messages to reach and influence their target audience. There are several overarching themes the site uses to legitimize attacks on US and NATO forces.

- "Infidels and Apostate Forces": The group refers to US forces as the "Invader Infidel American Forces," and to NATO forces as the "Infidel Allied Forces." Similarly, the Afghan Army is referred to as the "Apostate ANA (Afghan National Army)." More recently, the group has become vocal about Pakistan as well, referring to it as the "US Puppet or Apostate Pakistan." The group denotes to itself as the "Islamic Emirate." These themes are used very frequently and consistently.

- "Muslim Victimization and Civilian Killings": The videos

posted on the site typically document scenes of alleged Muslim victimization, and pictures of alleged prisoners of war in US detention facilities. On March 18, 2011, the home page feature was, “The US Continues its Massacres,” claiming that US forces had attacked and killed 40 civilians and wounded 20. The words capitalized below are taken directly from the statement:³

A press release by the Islamic Jihad Union reported that, on March 17, 2011, the Invader Infidel Spy planes had conducted an attack on Muslims and killed 3 mujahedeen and 14 Muslim brothers. A new statement made today [March 18, 2011] says that the Invader Infidel American Spy Planes conducted another attack at the Digor Region later that same day; and that this attack was solely aimed at the CIVILIAN POPULATION. As a result of this attack, 40 Muslims from the CIVILIAN POPULATION have been killed, and 20 have been wounded. As such, it is noted that the Invader Infidel American Troops are continuing their CIVILIAN MASSACRES. ... The whole world should know that the Invader Infidel AMERICA and its puppet Apostate PAKISTAN, are conducting CIVILIAN MASSACRES in the North Waziristan Tribal Areas.

The same theme was in a posting on March 9, 2011, entitled, “Invader Infidels are KILLING CIVILIANS.”⁴ The “Muslim victimization” theme was present in older statements as well. Their statement claiming responsibility for the March and April 2004 attacks in Uzbekistan, claimed that Muslims were being “tortured and imprisoned as a way to terrorize and degrade them.”⁵ Videos on the site carry such titles as “Scenes from Abu Ghraib” and “What Democracies Have Done to Mujahedeen.” The site also exploits statements and pictures about Guantanamo, which it keeps current and accessible.

• The concept of “Martyrdom”: A natural extension of the “Muslim victimization” theme is the message that those who attack “infidel” US or NATO forces are “heroic martyrs.” Attacks are often described as revenge or retaliation. The message is that Muslims have an “individual obligation” to defend other Muslims who are under attack. As such, those who fulfill this obligation become “martyrs.” The site publishes profiles of those who have conducted suicide attacks as having fulfilled the most noble role. These articles extol the bomber’s



Figure 3. Islamic Jihad Union Fighter
Source: sehadetzamani.com

“martyrdom” and hold them up as role models. This appears to be a tool aimed at foreign recruitment and to send the message that this is the greatest thing that a Muslim can do for “Allah.”

- “Jihad is Enjoyable and Appealing”: This is targeted at potential recruits. The videos, statements and interviews send the message that there is an atmosphere of brotherhood, camaraderie and strength in the jihadi training camps (Figure 3).
- “The Mujahedeen are Winning”: Videos showcase supposed victories and carry such titles as “Scenes of Azeri Mujahedeen Brothers” and “Show from an Iraqi Mujahedeen Brother,” claiming they are conducting bombings on US or NATO bases in Afghanistan. The site posts almost daily statements on their

actions in various regions of Afghanistan, citing the number of “infidels” that they killed that day. On January 4, 2011, a posting claimed that, “The Apostates are disappearing One by One,” discussing how a Pakistani governor was shot to death.⁶ On July 26, 2010, they released a long list of action, each one detailing the number of troops killed from a NATO country. They also released a picture of a US soldier as one of the victims.⁷ Such lists are published periodically with the title, “Islamic Emirate Operations Report,” with the IJU logo attached to them.

- “Muslim Unity”: This message uses Islam as a unifying factor to attract radical Islamists from different countries. A home-page link includes an interview with a Turkish suicide bomber from Germany who attacked a NATO compound in Afghanistan in March 2008.⁸ Titled “Our Interview with our Brother Ebu Yasir El Turki from the Islamic Jihad Union Mujahedeen,” it includes a segment where the interviewer asks the suicide bomber what message he would like to send to Muslims in Turkey. His answer is, “Hopefully you will continue to support us both financially and through prayer....There is no nationalism in Islam....Don’t get confused with ideologies like democracy, secularism, and others and let’s not let them confuse our beliefs.”⁹



Young Child Indoctrinated with Jihad Training
Source: Google Images

• “Pakistan is a US Puppet”: Recently improved collaboration between the United States and Pakistan has led to the group becoming vocal about the Pakistani army. They have started referring to it as the “Apostate Pakistani Army,” or the “Puppet Pakistani Army,” implying that Pakistan is a powerless US “puppet,” that has turned its back on its Muslim identity. A March 10, 2011 posting titled, “Interview with Turkish Sniper Hamza Harbi,” promotes this message clearly. In response to a question as to why the Mujahedeen are treating the Pakistani army the same as the US army, Hamza Harbi says:

The Pakistani government and Pakistani Generals, who have been purchased by the US Army, are releasing their troops onto us. We don't want to fight the Pakistani army. But we react to their attacks against us. And this is exactly what America wants. We are aware of this and focus our attention on the Americans. But the Pakistani army, who have traded their religion for a small fee to the Americans, are attacking us like hungry dogs. We are merely defending ourselves against the Pakistani army, while counter-attacking the American army. We know that the Pakistani army's weaponry, equipment and salary are being supplied by America. But it is impossible for the Pakistani army to deal with the Mujahedeen. Even the world's superpower, the US hasn't been able to deal with the Mujahedeen.¹⁰

• “Generation Jihad”: One very ominous theme is “Generation Jihad,” which targets children and their parents. The IJU emphasizes through different methods. These include glorifying child suicide bombers, developing games idolizing those who detonate themselves amid “infidels,” developing cartoon images and portraying training camps for children, and publishing videos which target children to attack the US. The site also posts videos claiming to show the “next generation of mujahedeen in training to become “jihadists” or “martyrs,” ingraining the message of ‘individual obligation to fight against infidels’ from a very young age.¹¹

The training videos typically combine the recitation of Quranic verses with scenes of children in combat training. They portray militancy as a legitimate part of Islam and sends the message that madrassahs (Islamic schools) are good environments for Muslim children to learn how to put their combat skills into practice. The group aims to perpetuate their ideology through generations and across regions.

Claiming Responsibility for Attacks

In July 2004, the group claimed responsibility for almost simultaneous bombings against the US and Israeli embassies in Tashkent as well as the office of the Uzbek prosecutor-general, killing two and wounding several others. The IMU claimed responsibility for the attacks as protests against the Uzbek government’s support of the US and Israel, as well as support for Palestinian, Iraqi, and Afghan militants.¹² Following the attacks, the US State Department categorized the IJU, which is well known for its expertise in the use of explosives, as a “Specially Designated Global Terrorist” group.¹³

In a September 11, 2007 statement released on sehadetzamani.com, the group claimed responsibility for a foiled plot a week earlier in which German police had arrested two Germans and one Turkish citizen on suspicion of plotting to bomb the Frankfurt International Airport (Figure 4).¹⁴ However, the IJU stated that, contrary to press reports, the targets of the operation were the US Air Force base in Ramstein, Germany, and the US and Uzbek consulates in Germany. The IJU also warned of future actions against American and Uzbek interests, and called for the removal of the German Air Force base in Termez,



Figure 4. Islamic Jihad Union Press Release Video
Source: sehadetzamani.com

Uzbekistan.¹⁵ The 2007 foiled plot in Germany represented the organization’s first attempt to target a European country, and signaled its intentions to expand its target list to include Europeans.¹⁶

The statement confirmed that the action was linked to the IJU and that the suspects were part of the group’s German cell. It was unusual for a terrorist group to claim responsibility for a failed attack.¹⁷ One possible reason for this may have been to raise their standing among other militant radical Islamic groups. The group desired to be credited for a plot labeled by the media as being “Germany’s bloodiest act of terrorism.” The quantity of explosives found was more than that used in the 2004 Madrid and 2005 London attacks.¹⁸ By issuing the statement on September 11, the group was signaling their ideological affiliation with Al-Qaida.



Figure 5. Alleged Islamic Jihad Union Suicide Bomber
Source: sehadetzamani.com

On March 6, 2008, the group issued a statement claiming responsibility for an attack that took place on March 3, 2008. A suicide bombing in Afghanistan destroyed a guard post and wounded several NATO soldiers. The statement claimed that it was conducted with the help of the Taliban, and praised a Turkish suicide bomber for carrying out the attack (Figure 5). This statement represents a typical IJU statement and includes all of the aforementioned themes and messages:

On 3 March 2008, our Mujahid of the ISLAMIC JIHAD UNION has successfully carried out an operation against a military camp hosting Invader Infidels and Allied Forces in the Sabari Nation Valley in Afghanistan's Paktika Region. This Heroic Mujahid, with God's help, has attacked the Invader Infidel Army's Camp with a car loaded with 4.5 Tons of Explosives. According to witnesses and the Taliban

Mujahedeen, with whom we organized the operation, the Invader Infidel's Camp was completely destroyed. Following our operation, 5 helicopters continuously carried bodies out of the rubble. The number of soldiers who died in the camp was kept secret. According to witnesses and Mujahedeen, the bodies of at least 60 American soldiers and 70 Collaborator Afghan soldiers were carried. This operation was in retaliation to our recently Martyred Mujahid Sheikh Ebu Leys El Libi and other Martyred Mujahedeen. This operation was carried out by bold Cüneyt Çiftçi (Saad Ebu Furkan), who came from Germany but of Turkish origin, who traded his luxurious life for Heaven....In the coming days, we will release scenes from this operation and a video recording of our brother's last words to the Ummah [Islamic nation].¹⁹

Target Audience

The group appears to be conducting an intense public relations campaign through the Turkish language site, particularly aimed at recruiting ethnic Turks from Central Asia and/or Turkey, and possibly even the ethnic-Turkish Uyghur population in China. Ethnic Turks represent a potential target audience due to strong linguistic, ethnic and geographic affinity to Uzbekistan and Central Asian states, from which the IJU originated.

The organization uses propaganda to reach the Turkish diaspora abroad, particularly the large Turkish population in Germany. The postings and the video dialogues are in Turkish, but some members speak with a heavy German accent or in broken Turkish, suggesting that they are second-generation Turkish immigrants from Germany. One interview is recorded in both German and Turkish.²⁰

It is important to note that their target audience appears to

be those who are already attracted to militancy; i.e., the propaganda “preaches to the converted.” They do not appear to be trying to recruit random visitors to their site. On the contrary, they seem to appeal to both experienced militants who have fought elsewhere, or inexperienced militants who already believe in the cause and have the network and contacts who can enable them to actually join the group or provide financial support. Active, explicit recruitment is rare on the site.

The group is also appealing to Islamic youth, and possibly the parents of those children, through its “generation jihad” theme, which makes the children’s training camps look like an educational facility where children can go to learn about the Qur’an and gain valuable training.

Conclusion

Although the Islamic Jihad Union has not publicly stated its philosophy, history, or objectives, an interview with the alleged leader of the group, Ebu Yahya Muhammed Fatih, featured on Sehadetzamani.com provides some insight into its goals.²¹ The interview reveals that the group was formed in 2002 in opposition to the regime of Uzbek president Islam Karimov, but later expanded its goals to “uniting all oppressed Muslims under the banner of Islam and conducting ‘jihad’.”

Several facts can be deduced from their information operations. First, statements on the site indicate that they are opposed to the governments of the US, Israel, Germany, and Uzbekistan, and object in particular to US and Uzbek military and political policies which they claim “oppress Islam and Muslims.”²²

Second, the group has shifted its focus from the Uzbek regime to a more general message of “jihad,” and “Muslim unity,” to cast itself as part of the global jihad and attract more foreign



IJU Militants Detained in North West Pakistan

Source: Google Images

recruits. This appears to have been an effective strategy. While the IJU's initial members were mostly Uzbek, the nationalities of those involved in the thwarted plot in 2007 suggest that it has expanded its recruits beyond Uzbeks to include Turks, and the Turkish diaspora in Germany.²³

Third, the group is attempting to ensure that their war will continue to be fought by successive generations, through its themes and messages which are likely attractive to uneducated youth with no real life prospects and their parents.

Fourth, the IJU has been cooperating with the Taliban in Afghanistan; and has links with Al-Qaida, at least ideological, if not operational and financial. The group's operations focus on US and NATO forces in Afghanistan; the Afghan National Army and more recently, the Pakistani Army. The group adapts its targets according to changing political and military circumstances, possibly to deter other forces from collaborating with the US and NATO forces in Afghanistan. This is reflected in their messages.

Fifth, each time the IJU has announced forthcoming actions, they follow up with bombings or foiled attacks, demonstrating some competence as a functioning terror network.²⁴ In April 2007, the group announced that it would step up actions abroad, leading German officials to issue a warning and increase security around its embassies. Five months later, the group attempted to attack US and Uzbek targets in Germany. Their threats are credible, and this points to the need to closely monitor the site.

Finally, their themes and messages reveal vulnerabilities that can be exploited. Each of their themes can be countered with messages such as the Islamic injunction against suicide, or highlighting negative experiences of surviving suicide bombers. A thorough examination of their messages reveal the kinds of information operations that the US and the DoD can conduct to neutralize or at least minimize the effect of the IJU's messages. This would undermine their credibility as well as other militant radical Islamic groups who use the same messages in their public relations campaigns. 🌐

Endnotes:

1. "Islamic Group Claims Uzbekistan Attacks," JihadWatch.org, April 12, 2004; <http://www.jihadwatch.org/archives/2004/04/001535print.html>. 2. Crawford, David. "Web Sites for Germany's Turks Fuel Fear of Homegrown Terror," *The Wall Street Journal*, September 13, 2007; <http://online.wsj.com/public/article/SB118964547572825925.html>.
3. "Amerika Katiliama Devam Ediyor (The U.S. Continues its Massacres)," *Sehadetzamani.com*, March 18, 2011; http://sehadetzamani.com/haber_detay.php?haber_id=2444.
4. "İsgalci Kafirler SİVİLLERİ ÖLDÜRÜYOR (Invader Infidels are Killing Civilians)," *Sehadetzamani.com*, March 9, 2011; http://sehadetzamani.com/haber_detay.php?haber_id=2435.
5. "Islamic Group Claims Uzbekistan Attacks," JihadWatch.org, April 12, 2004; <http://www.jihadwatch.org/archives/2004/04/001535print.html>.
6. "Mürtedler Bir Bir Yok Oluyor; (The Apostates are Disappearing One by One)," *Sehadetzamani.com*, January 4, 2011; http://sehadetzamani.com/haber_detay.php?haber_id=2413.
7. "İslam Emirliği Operasyon Raporu (The Islamic Emirate Operation Report)," *Sehadetzamani.com*, July 26, 2010; http://sehadetzamani.com/haber_detay.php?haber_id=2385.
8. "Bavarian Cüneyt Çiftçi is Germany's First Suicide Bomber," *The Sunday Times*, March 18, 2008; <http://www.timesonline.co.uk/tol/news/world/europe/article3571785.ece>.
9. "İslami Cihad İttihadi Mücahidlerinden Ebu Yasir El Türki Kardeşimiz İle Gerçekleştirdiğimiz Röportajımız (Interview with Ebu Yasir El Türki of the Islamic Jihad Union Mujahideen)," *Sehadetvakti.com* April 14, 2008; http://www.sehadetvakti.com/haber_detay.php?haber_id=1907.
10. "Türk Sniper Hamza Harbi ile Röportaj (Interview with Turkish Sniper Hamza Harbi)," *Sehadetvakti.com*, March 10, 2011; http://sehadetzamani.com/haber_detay.php?haber_id=2438.

11. "Geleceğin Şeyhleri (Sheikhs of the Future)," *Sehadetvakti.com*, August 18, 2007; http://www.sehadetvakti.com/haber_detay.php?haber_id=1565.
12. Samigullina, Alia. "Business of Shabak," *Politika*, August 10, 2004; http://www.gazeta.ru/2004/07/31/oa_128728.shtml.
13. "U.S. Department of State Designates the Islamic Jihad Group Under Executive Order 13224," U.S. Department of State website state.gov; May 26, 2005; <http://merln.ndu.edu/archivepdf/terrorism/state/46838.pdf>; Landler, Mark and Nicholas Kulish. "Police Arrest 3 in German Terror Plot," *International Herald Tribune*, September 5, 2007; <http://www.ihf.com/bin/print.php?id=7393593>.
14. "Terör Saldırısında Şüpheli Türk Genç (Suspicious Turkish Youth in Terror Attack)," *Sabah*, September 6, 2007; <http://www.sabah.com.tr/2007/09/06/haber;4194354E1AF7440487CB8815A9842086.html>.
15. "İslami Cihad İTTEHADİ" Basın Açıklaması... ("Islamic Jihad Union" Press Release...), *Sehadetvakti.com*, September 11, 2007; http://www.sehadetvakti.com/haber_detay.php?haber_id=1587.
16. "Germany: Authorities Say Uzbekistan-Based Group behind Terrorist Plot," *Radio Free Europe*, September 6, 2007; <http://www.rferl.org/featuresarticle/2007/09/6ec8adad-f98f-413d-95e1-776074d74a24.html>.
17. During raids in Germany following the plot, police also found an IJU manual for bomb making. Saidazimova, Gulnoza. "Germany: Authorities Say Uzbekistan-Based Group behind Terrorist Plot," *Radio Free Europe*, September 6, 2007, *Ibid.*; and Laabs, Dirk. "German Case Offered Alleged Earful," *LATimes.com* September 8, 2007; <http://www.latimes.com/news/nationworld/world/la-fg-plot8sep08,1,6897745.story?ctrack=3&cset=true>.
18. "Terrorist Plots in Europe: Foiled, This Time," *The Economist*, September 6, 2007; <http://www.economist.com/node/9769480>.
19. "İslami Cihad İttihadi BASIN AÇIKLAMASI (Islamic Jihad Union PRESS STATEMENT)," *Sehadetvakti.com*, March 6, 2008; http://www.sehadetvakti.com/haber_detay.php?haber_id=1889.
20. "In der Westlichen Presse wird ja der Islam als Terrorismus dargestellt. Es wird ja behauptet das di (Our Interview with the Islamic Jihad Union Mujahideen Abdulgaffar El Almani)," *Sehadetvakti.com*, May 23, 2008; http://www.sehadetvakti.com/haber_detay.php?haber_id=1921.
21. "İSLAMİCİHAD İTTEHADİ Emiri EBU YAHYA MUHAMMED FATİH ile Röportajımız (Our Interview with the Amir of the ISLAMIC CİHAD UNION, EBU YAHYA MUHAMMED FATİH)," *Sehadetvakti.com*, May 31, 2007; http://www.sehadetvakti.com/haber_detay.php?haber_id=1202.
22. According to Uzbek and international human rights groups, thousands of religious Uzbek Muslims have reportedly been jailed in recent years for practicing Islam outside government-sanctioned institutions. The statement from the Islamic Jihad Group that claimed responsibility for the March and April 2004 attacks in Uzbekistan, also claimed that Muslims were being "tortured and imprisoned as a way to terrorize and degrade them." "Islamic Group Claims Uzbekistan Attacks," *Jihad Watch.org*, April 12, 2004; <http://www.jihadwatch.org/archives/2004/04/001535print.html>; and "İslami Cihad İTTEHADİ" Basın Açıklaması... ("Islamic Jihad Union" Press Release...), *Sehadetvakti.com*, September 11, 2007; http://www.sehadetvakti.com/haber_detay.php?haber_id=1587.
23. Schmitt, Eric. "Europeans Get Terror Training inside Pakistan," *New York Times*, September 10, 2007; http://www.nytimes.com/2007/09/10/world/europe/10germany.html?_r=1&oref=slogin.
24. "Uzbek Terror Networks: Germany, Jamaat and the IJU," *The Jamestown Foundation*, November 8, 2007; [http://www.jamestown.org/programs/gta/single?tx_ttnews\[tt_news\]=4533&tx_ttnews\[backPid\]=182&no_cache=1](http://www.jamestown.org/programs/gta/single?tx_ttnews[tt_news]=4533&tx_ttnews[backPid]=182&no_cache=1).



Ms. Karen Kaya is a Middle East / Turkey Analyst for the Foreign Military Studies Office, located in Fort Leavenworth, KS.

She earned her Master of Arts degree in International Relations from Brandeis University, and has worked as a linguist and defense policy analyst for the US government.

Structuring Tactical Military Information Support Operations for Low-Intensity Conflict

By
LTC J.R. Reiling, US Army

Editor's Note: LTC J.R. Reiling's experience in tactical MISO and his views on the make up of a team is insightful. The blend of ability to operate in a low intensity yet high threat environment to lightly armed soldiers is a real problem for MISO mission effectiveness. Force protection is a concern that commanders will always enforce first. Hence LTC Reiling's suggestion here on enhancing the tactical MISO team.

Introduction

Military Information Support Operations (MISO) has an opportunity to review its doctrine and organization to better reflect the current unconventional environment in which the US Army is engaged. One possible area for improvement could be resizing the tactical MISO team to increase the number of both personnel and vehicles, enhancing the team's effectiveness.

Background

For half a century after WWII, US Army training, equipping, planning, exercising and doctrine was based upon what strategists considered the "Most Dangerous Course of Action" in terms of potential threats to US national security: an all-out assault by Warsaw Pact armed forces along the "Iron Curtain." Our prudent preparation for this eventuality so deeply

embedded itself within the US Army that even ten years after commencement of the Global War on Terror, soldiers still encounter organizations or procedures more appropriate for battling the Soviet Union.

The current US Army MISO force structure may exhibit characteristics of this "Fulda Gap" thinking. Currently, a Military Information Support Team (MIS Team) comprises of three Military Occupation Specialty (MOS) 37F, or Psychological Operations (PSYOP), soldiers (see Figure 1) and one M-1114 HUMVEE with loudspeaker. This makes sense when placed in the context of the expected mission in a conventional conflict similar to that described above. In this case, the team would be riding on the friendly side of the lines broadcasting into enemy-held territory, or operating in conjunction with advances by US forces. Force protection considerations would not be above and beyond those for any other operational or support forces. Put bluntly, the loss of a few MIS Teams during high-intensity conflict would be considered part of the cost of conducting decisive operations.

Analysis

Unlike a WWII or Desert Storm scenario, a low-intensity conflict (LIC) environment turns MISO into one of the highest-risk of the US Army forces. Now these small and lightly-armed



US PSYOP Soldiers and Iraqi Policeman Prepare to Conduct Leaflet Distribution

Source: defenseimagery.mil

DOORS ARE NOW OPEN...

Come on In!

The Joint Information Operations Assessment Clearing House is a repository for joint IO assessment knowledge supporting the joint IO assessment community. It contains assessment techniques, artifacts, and resulting data aiding in cataloging and evaluating information-related capabilities intended and actual effects based on combatant command mission objectives. The Joint Information Operations Assessment Clearing House enables the joint IO force to capitalize on existing capabilities and joint planning methods to provide informative data resulting from joint IO assessment.



Following a tour at the service college, an Air Force Major is dispatched to the Korean peninsula for the payback, joint tour. Checking into the combatant command, the Major learns the assignment is to the Information Operations (IO) Division. The assignment makes sense. The Major is an Electronic Warfare Officer; however, the Major will lead the newly formed IO Assessment Branch. Well equipped to staff EW issues, the Major has no training, education, or experience in information operations assessment. Our Electronic Warfare Officer is concerned upon hearing assessment is “a big deal.”

An Intelligence Analyst, assigned to the combatant command J2, sees command interest in IO assessment growing. As a member

of the Information Operations Intelligence Integration community, our intelligence analyst knows how to generate an intelligence assessment, but assessing the effectiveness of U.S. information operations – that’s

“New clearing house enables collaboration on IO assessment between the CCMD’s, Services and Joint Staff.”

different. It’s difficult enough working with operators in developing requests for information regarding the adversary. Imagine the challenge of gathering intelligence that speaks to the efficacy of U.S. information operations, never mind that some of the needed information may lie outside the traditional “INTs.”

In this era of increasing emphasis and urgency regarding assessment,

our Electronic Warfare Officer’s and Intelligence Analyst’s experience are not unique. They are representative of the growing number of professionals whose IO assignment or job involves less IO and more IO assessment. These professionals are aware of the growing importance placed on assessment and may feel ill-equipped to conduct assessment activities. Their professionalism motivates them to “get smart” on assessment; however, their dilemma is where do they receive the assessment training or education?

Our Electronic Warfare Officer and Intelligence Analyst need to learn about the many facets (e.g., best practices, community of interest, lexicon, references) of IO assessment. They need gouge. Behold the... JOINT IO ASSESSMENT CLEARING HOUSE!



JOINT INFORMATION OPERATIONS

Assessment Clearing House

intelinkshare.intelink.sgov.gov/sites/jiowc/assessments

teams are frequently operating alone or in conjunction with other small forces (such as a Civil Affairs team or an infantry patrol), often in areas not regularly covered by other US forces. This increased vulnerability is occurring in the context of a LIC environment wherein casualties are more keenly felt by US leadership attempting to maintain public support for the operation.

Force protection (FORCEPRO) requirements to travel “outside the wire” in the LIC environment we operate in today have evolved to a consistent two-vehicle, four-person minimum. The current MIS Team comes up one short in both areas, forcing it to cast about for reinforcement in order to perform its job. On a major forward operating base, this is an inconvenience, but not impossible to overcome. The motor pool can usually come up with another vehicle, and you can always find service members happy to get off the compound for a few hours who will even trade for the privilege (the surest way to get your vehicle first-aid kit up to standard and beyond is to invite a medic from the clinic to accompany you on a mission).

It is a different story when operating with special operations forces. In this situation the MIS Team is in an austere environment where almost everyone else frequently leaves the camp on an irregular battle rhythm including nighttime. These

soldiers will have less incentive to accompany the MIS Team on missions above and beyond their demanding workload. The MIS Team may be well-integrated into the operational missions conducted by their host team. However, they often have problems trying to get support to get out and conduct the routine patrolling and interaction critical to conditioning the local population in order to make future operations more successful.

Proposal

A new MIS Team organization and equipment could include (see Figure 2):

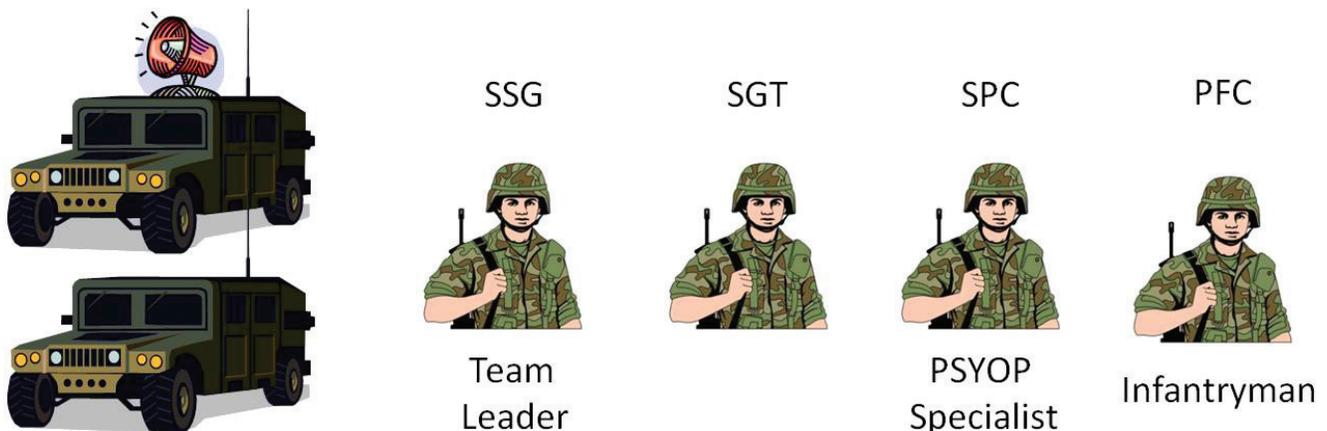
- 3 x 37F MISO specialists
- 1 x 11B Infantryman
- 1 x M1114 with loudspeaker
- 1 x M1114

A dedicated second vehicle would increase the MIS Team capability by allowing them to stage newspapers, novelty items and other things normally disseminated to target audiences during patrols. Reserve ammunition, fuel, food and other stocks can also be laid in rather than being loaded and unloaded from borrowed vehicles for every mission.

Figure 1 - Current Tactical MISO Team



Figure 2 - Proposed Tactical MISO Team



Like the second vehicle, a fourth team member would enable the MIS Team to meet FORCEPRO minimums in a LIC environment. While on patrol, the fourth team member would assist with vehicle security and/or overwatch for the remaining team members (necessary missions in a LIC environment which are not as strongly emphasized in a conventional conflict), increasing the MISO capability of the MIS Team. An 11B would be the best MOS for directly bringing combat capability to the MIS Team. The infantryman would also be able to share their skill with other team members and increase the overall combat capabilities of the MIS Team.

An alternative would be to simply provide the MIS Team with an additional MISO soldier, which would likely be the preferred option of the MISO community. However, the MISO force is currently badly undermanned and it is unlikely that the assignment and training pipelines will alleviate this shortfall in the foreseeable future. Giving each team an 11B would be a more realistic lower-cost option that still improves the overall capability and survivability of the MIS Team.

A reorganized MIS Team would be more expensive to deploy and maintain due to the increase in personnel and equipment. However, this should be measured against the opportunity cost gain from MISO practitioners no longer having to spend time in a combat operations zone securing and integrating the resources needed to conduct their mission, or cases of MIS Teams at austere locations not being able to conduct their mission at all. The larger structure would correspondingly result in an increase in time available to the MISO specialists to plan and execute their primary mission.

Conclusion

The force restructuring described above could prove to be a means to field MISO forces better suited for a LIC environment than the current organization. It would enable MISO to deploy

ready to support any host organization it is assigned to, and be better able to operate and survive in a LIC environment.

In the event of a future major conventional conflict, MISO forces restructured as discussed above would no longer be optimal for the operational environment. In fact, they would be exhibiting what may then be known as “Anbar Province” thinking.

References

Information on current MIS Team organization and equipment taken from US Army Field Manual 3-05.302, “Tactical Psychological Operations Tactics, Techniques and Procedures” 28 Oct 2005 as well as undated usage guide “PSYOP vs MISO” published by the MIS Directorate, U.S. Army John F. Kennedy Special Warfare Center and School. MIS Team figures derived from Figure 2-5 “Tactical Psychological Operations detachment” of USA FM 3-05.302.



LTC J.R. Reiling (USA) served as a Psychological Operations officer in the 4th Psychological Operations Group at Fort Bragg, NC from 2003 through 2005 and is currently assigned as a Military Information Support Operations instructor at the Joint Forces Staff College, Norfolk, VA.



US Tactical MISO Team with Vehicle and Loudspeaker
Source: defenseimagery.mil

Evolution of Information Operations Intelligence Integration

By
Mr. Joshua Cook

Editor's Note: Mr. Josh Cook is a staunch advocate of ensuring the intelligence community properly supports the IO fight. His hard work in organizing the IOII effort has made him the foremost authority on the community's evolution. His contribution on this subject is very important to this issue of *IO Sphere*.

“...the vast intelligence apparatus is unable to answer fundamental questions about the environment in which U.S. and allied forces operate and the people they seek to persuade. Put simply, the IC has the tendency to overemphasize detailed information about the enemy at the expense of the political, economic, and cultural environment.”

The authors of the above quote are talking in general about a focus on threat-centric intelligence vs. population-centric intelligence. Lieutenant General Michael Flynn (US Army), Captain Matt Pottinger (US Marine Corps), and Mr. Paul Bachelor in their report *“Fixing Intel: A Blue Print for Making Intelligence in Afghanistan Relevant”* propose that intelligence is often focused on things rather than people. Their arguments resonate particularly well with the Information Operations Intelligence Integration (IOII) community. Namely, IOII fuses vitally needed all-source information environment (IE)-centric data, to include friendly, adversary and, equally important, neutral intelligence and information. In this article, we will explore activities undertaken by the IOII Community of Action (COA) to ensure intelligence personnel dedicated to supporting IO are in the right place and possess the right skill sets to provide exceptional intelligence products and analysis to IO planners.

The IOII COA has come a long way toward that goal since the 2009 Intelligence Support to Information Operations

(ISIO) study, released by the Office of the Undersecretary of Defense for Intelligence (OUSD-I), which called for a normalization of the ISIO force. That year, to address issues facing our community, as well as showcase the integrative nature of our work, we shifted our identity from the ISIO Community of Interest to the IOII COA. The 2011 Secretary of Defense memo changing the IO definition to reflect IO as an integrating strategy falls in line with how the intelligence personnel assigned to support IO planners have viewed their job for some time. This paradigm was announced at the 4th Annual IO Intelligence Conference in 2009, and later codified by Lt Gen John C. Koziol, Deputy OSD-I, for Joint Coalition and Warfighting Support, in a June 2009 memo. Seeking membership and participation from across the Department, the IOII COA's first task was to address initiatives within the Defense Intelligence Guidance for FY11-17, which established IOII as a priority for the Defense Intelligence Enterprise. Through these actions, we have addressed IOII-related issues in doctrine, training, and force development.

Over the past three years, we have worked to codify our beliefs and principles by influencing key Department of Defense (DOD) guidance. DOD Directive (DODD) 3600.01, Information Operations, now states, “the IO force are military professionals in the Active, Guard, and Reserve Components; DOD civilian professionals; and select academic and contract personnel who directly support the integration of IO. The IO force consists of information-related capability specialists, IO planners, and intelligence personnel dedicated to supporting IO.” The takeaway here is that, although we have our own set of issues and processes, intelligence personnel are considered part of the IO force and are key to successful IO. Additionally, DODD 3600.01 directs OUSD-I to craft a DOD instruction regarding IOII. This will further codify the COA and its work in upcoming years. With regard to joint publications (JP), JP 2-01.3, *Joint Intelligence Preparation of Operations Environment*, now discusses the central IOII activity of information-environment characterization. And, for the first time ever, the information operations community recognized definition of IOII as “the integration of intelligence disciplines and analytic methods to characterize and forecast, identify

Online IO Training Available on SIPRNet

JIOWC has developed training scenarios with the intent of providing basic Information Operations “skills-based” training in an online, self-paced environment. The scenarios are designed to exercise critical thinking on the part of the participant. They also strive to demonstrate, whenever possible, *Best Practices* in the “integration of Information-Related Capabilities with other Lines of Operation” (*Information Operations*).

To see how Information Operations might be used when:

- the death of a world leader coupled with a poor harvest leads to the economic collapse of a nuclear state, or
- a volcanic eruption in a highly populated developing nation puts an entire city at risk, or
- an unstable theocracy finally realizes its goal in developing WMD

Go To SIPRNet at:

www.intelshare.intelink.sgov.gov/sites/jiowc/Divisions/j5/J57/IOCBT/Online_Training.aspx

For more information contact: IO_CBT_Feedback@jiowc.smil.mil



JOINT ELECTRONIC WARFARE THEATER OPERATIONS COURSE



SAN ANTONIO, TEXAS

A joint certified course created to develop Electronic Warfare planning, coordination, and integration skills for personnel in direct EW support to Joint Force Commanders and to enhance corporate EW knowledge for the joint force. For more information call 210-977-6238 (DSN 969) or E-mail: jewc.eww.training@us.af.mil.

vulnerabilities, determine effects, and assess the information environment” has been widely accepted.

With regard to training, we recognized basic and advanced IOII knowledge, skills, and abilities (KSA) at the 4th Annual IOII conference in 2009. Taking these forward to the 5th Annual conference, we addressed shortfalls in the advanced IOII training arena by identifying advanced-level IOII training objectives and developed a course curriculum to tackle these training needs. Those efforts were consolidated and refined at the 6th Annual IOII conference, and as a result, the rest of 2011 was spent garnering joint certification for Defense Intelligence Agency’s (DIA) ISIO course that teaches to the basic KSA level. Our 2011-2012 efforts focus on developing, validating through a pilot course, and certifying what has become the IE Advanced Analysis (IEAA) course that will teach to the advanced IOII KSA level. The joint certifications these courses have allow IOII skilled analysts to be identified (via the training requirements) against intelligence professionals dedicated to supporting IO planners.

At the 6th Annual IOII conference, the workforce identification working group, and subsequently a larger cross-section of conference attendees, agreed that there should not be an IOII force with special occupational identifiers (e.g., military occupational specialties, Air Force specialty codes) or special experience identifiers etc. Rather, intelligence professionals supporting IO planners should be trained in IOII based on the KSAs and emerging training requirements identified above. The 7th Annual conference force development working group took information from a data call that identified these billets and attached training requirements to them. The training requirements (i.e., DIA’s ISIO course, the Joint Information Operations Planner’s Course, and IEAA) are now being reviewed before formal submission. Also during the 2012 conference, we refined IOII-related universal joint tasks (UJT) under the IO mission grouping to ensure those assigned to

perform the IOII function have appropriate evaluation criteria in place. Those recommendations will go forward as a part of an update to IO UJTs at large.

Through the hard work of the IOII COA in the areas of doctrine and force development (training, education, and force management), we have made noteworthy progress in normalizing IOII at the joint level. That is significant in that we are the ones who will provide the IE baselines IO planners will utilize to narrow their planning efforts and set up the assessment of their activities. We will build out the joint intelligence preparation of the operational environment products that describes adversary capabilities in the IE. We will work with the broader J2 community to ensure collection plans and assets are in place to inform the measure of effect and help adjust the plan accordingly. The work of the COA benefits the whole IO force because, after all, IOII allows operations and intelligence to achieve a mutual understanding of and the interrelationship among the physical, information, and cognitive dimensions of the IE. 🌐



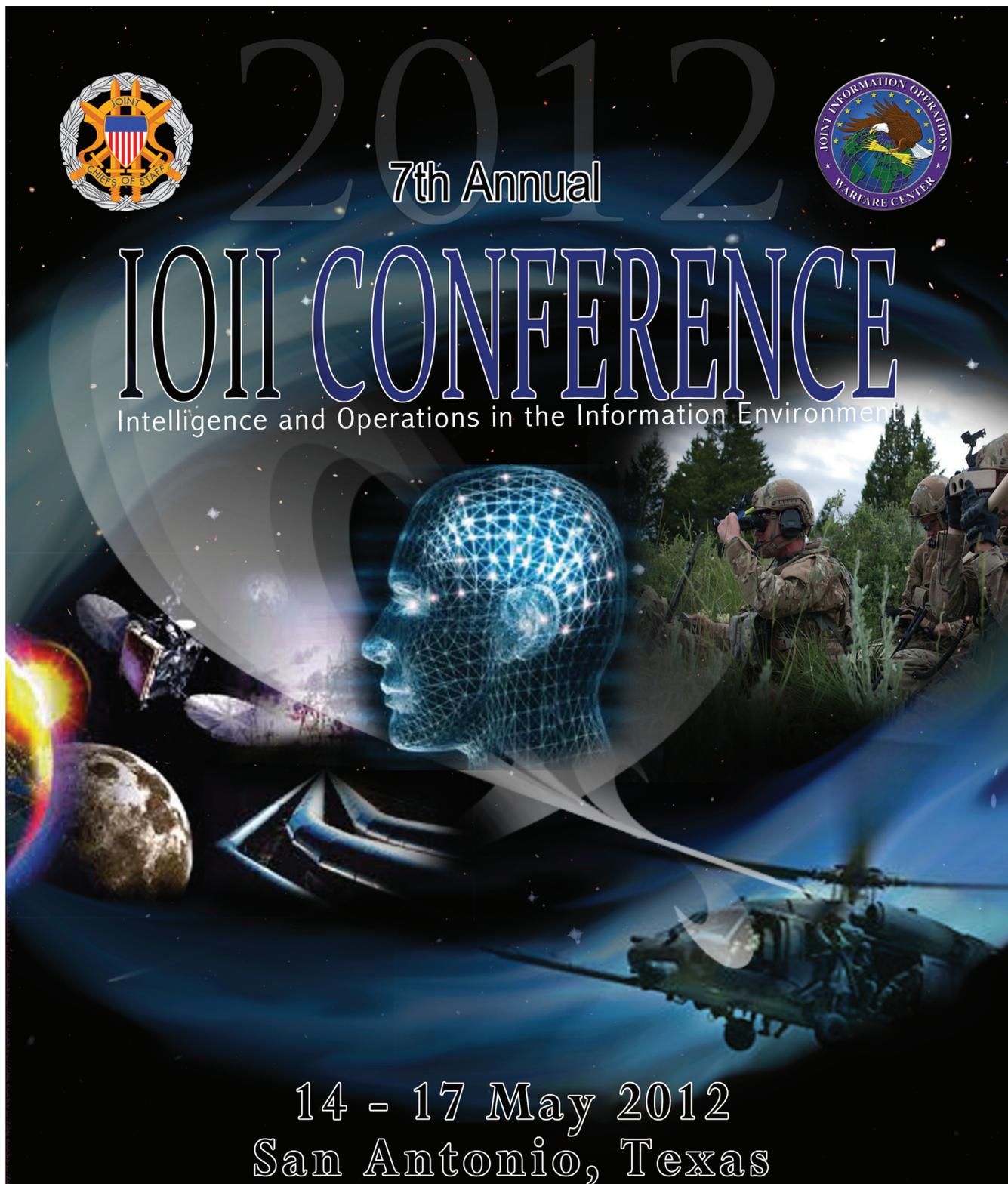
Mr. Joshua Cook is an Intelligence Analyst at the Joint Information Operations Warfare Center in San Antonio, Texas. He has been a dedicated advocate for IOII and ensuring the IC was focused on intelligence that is dedicated to effective information-related activities.



US Army Soldier and Linguist Conduct Interviews to Gather Intelligence in Afghanistan

Source: defenseimagery.mil

Thank You to Everyone Who Participated in 2012
For Information on the 2013 IOII Conference Contact
Mr. Josh Cook at joshua.cook@us.af.mil



2012
7th Annual
IOII CONFERENCE
Intelligence and Operations in the Information Environment

14 - 17 May 2012
San Antonio, Texas

IO Sphere Transition to the Digital Age

San Antonio, TX-(September 15, 2012) The IO Sphere will no longer be issued in print form after this issue. This is part of a DOD initiative to reduce the cost of print journals. In trying to make the transition as easy as possible and provide our readers the most flexibility, the IO Sphere editorial staff has been researching getting the IO Sphere into as many digital reading venues as possible.

One of the main thrusts of this effort is to get IO Sphere published in a format that allows use on most available e-reader hardware and e-reader applications on Apple and Android products. The only e-reader platform we currently are not supporting is Microsoft as they have terminated their e-reader software earlier this year. The capability exists to support, so we are willing to relook at Microsoft if there is sufficient demand. Digital versions for use on e-reader platforms will be available starting with this issue and should be released and available within a week or two following release of the print version.

As each platform is different, there are a variety of methods for loading the IO Sphere on the platform of your choice. There will be three digital versions of the IO Sphere: .mobi, for use on Kindle products and apps; ePub, for use on most other e-reader platforms and apps including Nook and iBooks; .pdf for reading on the computer, but more importantly, for printing.

iPad is probably the easiest platform for loading the IO Sphere. If you have the Kindle app, you can choose whether to download the ePub or mobi version as both will work. Simply download the version you prefer and tap the IO Sphere icon. iPad will give you the choice of app, either iBooks or Kindle depending on the version you downloaded. Tap your choice and the IO Sphere will open in the application for reading.

Other tablets create a problem providing straight forward instructions for loading the IO Sphere as there are dozens, if not hundreds, of different tablets all coming pre-loaded with different applications. Many, perhaps even most, of these tablets may work in the same way as with the iPad, but there is no way to test all of the various tablets to see if this is actually true. Since both Android and Windows tablets, with the exception of the e-reader pseudo tablets (Nook Color, Nook Tablet, and Kindle Fire), can load a Kindle app, the surest method of loading the IO Sphere is to e-mail the .mobi file to your tablet's Kindle app. Kindle also has a fairly easy method for loading the IO Sphere on your device or app. Every Kindle has a unique e-mail address. You simply e-mail the .mobi file to your Kindle address and it will automatically load into the device or app next time it's connected to a network. Conversely, if you provide your Kindle e-mail address to the IO Sphere editorial team, we can e-mail the .mobi file directly. In order for this to work, you must update your Kindle Approved Personal Document E-mail List to include the e-mail address sending the IO Sphere. The e-mail you created your Kindle account with is automatically on the list. Complete instructions for doing this can be found in Kindle support and will also be posted in the same folder as the .mobi files. You can also sideload the IO Sphere into your Kindle hardware. The procedure is essentially the same as with the Nook below.

Nook isn't quite as easy as either of the other two options, but also isn't all that difficult. The procedure for loading personal content on Nooks is called "sideloading." To do this, download

the ePub file to a computer you can plug your Nook into. Plug in your Nook and browse to the Files folder. Inside that folder you will find various sub-folders for books, magazines, and documents; save the IO Sphere into the folder you prefer. Safely remove your Nook hardware and you are ready to open the journal as you would with any other Nook content.

IO Sphere will be mailing out post cards to all the subscribers on the new digital distribution with more information. If you have any questions please contact the editor at jiowc.iosphere@us.af.mil.



Tendency Analysis

By

Mr. Mark W. Conder

Editor's Note: Tendency analysis is an important aspect of IOII. The need to be able to gain information and intelligence from trends and tendencies is critical to gaining insight into culture and human factors that make up attitudes and beliefs. Information-related activities in support of traditional military operations are dependent on this type of intelligence analysis.

What is “Tendency Analysis”? Some schools of thought will describe tendencies as being nuanced observables in an environment that tip off somebody that something is about to occur. I have also heard it described as something small that tells a soldier to not go down a particular alleyway. The nuanced observables used in these descriptions of tendency analysis are described as working on the sub consciousness of the observer.¹ However, this is not really tendency analysis, but rather anomaly analysis on the minute scale, and how minute anomalies register on the human brain and manifest within our perceptions and thoughts.

To understand tendency analysis, first we have to look at what the definition of tendency is as it relates to information operations and influencing people – “a proneness to a particular kind of thought or action.”² What this definition shows us is that people will have a particular fondness for, or a pattern to, a preferred way of thinking or actions/reactions to stimuli. In other words, people will have a preferred pattern to how they think and how they will react to a given situation.

Tendency analysis, therefore, is the effort to truly get inside an adversary's thought and decision-making process to set the cognitive conditions for them to make the decisions we desire them to make to do the actions/reactions we desire them to do. To illustrate some of these principles, we can examine three examples: a sports analogy, an example from pop culture, and a historical military example.

The sports analogy is a basketball game, and the focus is the match-up between the point guards on each team. In this example, the reader is the one of the point guards observing the other. The specific observations of the opposing player are that he dribbles the ball predominately right handed and shoots right handed. The logical conclusion is that he is right-handed. . . Being right-handed, it can be assumed that he is going to have a preference or tendency to go his strong side: the right. This can be confirmed through the initial observations on the court within the first few minutes of the game. Knowing the tendencies of the opposing right-handed player, the observer can now set conditions by providing subtle observable behaviors, such as body position and floor position, to either lure the opposing player into a trap set on his strong side, or force him to go to his weak side.

A classic Hollywood example appears in the movie “Patton,” when George C. Scott, as Patton, declares after his forces defeat German forces in North Africa under the presumed command of German Field Marshal Erwin Rommel, “Rommel, you magnificent bastard, I read your book!” While this movie quote and scene cannot be attributed as authentic, it does highlight a principle of tendency analysis. The scene hints that Patton had studied Rommel's writings and learned how Rommel thought, and acted/reacted under certain conditions. Patton knew his adversary.

This becomes a major component of tendency analysis: getting to know as much about how the adversary thinks and reacts to certain stimuli when making decisions.

Pattern analysis is also an integral feeder component for tendency analysis. By examining the patterns of decision making as revealed through behaviors and actions/reactions to environmental stimuli, the tendencies of the decision makers

THE IO LIBRARY

Joint and Service IO Doctrine, Policy, and More

A Complete One-Stop Shop For All IO References

On SIPRNet: <http://www.intelink.sgov.govsites/jiowc/home.aspx>

**On the Internet Via APAN at:
<https://community.apan.org/ioc>**

A GLOBAL IO COMMUNITY RESOURCE

ADVOCACY FOR IO



can be revealed and taken advantage of. A classic military example of the application of pattern and tendency analysis can be seen in the 206 BC Battle of Ilipia, near modern day Seville, Spain, between Roman forces under Scipio Africanus and Hannibal's Carthaginian forces under the command of Hasdrubal and Mago Barca. On the first day of engagement, Hasdrubal and Mago attacked the Roman forces immediately upon arriving on the battlefield; however, Scipio's tactics and forces were able to throw back this initial assault. Over the next few days, observed the patterns that betrayed the mindset of his opponents. Scipio noted that the Carthaginian commanders always fed their forces at a certain time of day, took to the field at a certain time, showed a preference for favored formations, and react to a given situation in the same manner. Scipio always took the field after the Carthaginians and always presented the same formation: the legions in the center and the Iberian forces on the wings. In doing so, Scipio set a pattern of response and habit that he wanted them to perceive.

On the morning Scipio decided to attack, fed his forces earlier than normal; before daylight. He then moved them forward toward the enemy encampment, waiting until they were closer to form up their battle formations. He changed the arrangement of forces by placing his stronger legion forces on the wings and the weaker Iberian forces in the center. Attacking before daylight, the Carthaginians were caught off guard and found themselves having to quickly arm and rush into battle unprepared. As expected, the Carthaginian commanders formed up their forces in their preferred formations, expecting Scipio to have done the same. However, now Scipio's stronger forces were able to collapse the wings of the opposing forces and hammer their flanks.³

While we can never know exactly what was in the mind of Scipio, his battle strategy and his maneuver tactics show he used pattern-analysis thought processes to determine the tendency of his enemy's decision making, and adjusted his actions accordingly to present a deceptive picture of his own tendencies.

Going back to our original example in the beginning of this paper of anomaly analysis, we can now see that anomaly analysis and tendency analysis, both dependent upon pattern and trend analysis as information feeders and human factors analysis to know the enemy, are different sides of the same coin. From our perspective, we want to learn the tendencies of our adversaries to influence their decision making process. On the other side of the coin, we want to look for anomalies within our environment to analyze them to reveal not only potential enemy actions, but also to take advantage of our own tendencies. This area of analysis can be that line of effort that could turn the tables of a single engagement, affecting the outcome of larger battles across many dimensions of the conduct of warfare. 🌐

Endnotes:

1. Hall, Wayne. M. (2010). *Intelligence Analysis: How to Think in Complex Environments*. Santa Barbara: ABC-CLIO, LLC., page 205-2173.
2. Merriam Webster. (1999). *Merriam Webster's Collegiate Dictionary: Tenth Edition*. Springfield: Merriam-Webster, Inc.
3. Scullard, Howard. H. (1970). *Scipio Africanus: Soldier and Politician*. New York: Cornell University.



Mark Conder is a Sr. Counter-Terrorism Intelligence Analyst with the Joint Information Operations Warfare Center's SOCOM Intelligence Cell and a retired U.S. Army Intelligence Professional with over 22 years of experience. Mark, guest lectured at the Joint Special Operations University, teaches courses on terrorism, and has intelligence experience from the tactical to the national-level.



Coalition Human Terrain Analysis Team Conducts Women's Forum in Afghanistan
Source: defenseimagery.mil

Cultures and Organizations: How IOII Can Support Successful Non-Lethal Operations

By

Captain Gustavo A. Molina, US Army

Editor's Note: Non-Lethal Operations are largely operations that are centered around information-related activities. IO is a central part of those operations and almost all traditional military activities in the future will include significant operations that are considered non-lethal. These operations are dependent upon intelligence and proper intelligence integration. CPT Molina's experience in these operations is insightful.

The world is a beautiful place with a rich history full of diverse cultures in remote places. I have spent two, soon to be three, years of my life in Afghanistan interacting with the Pashtun people, traveling the same land Genghis Khan and Alexander the Great ruled. Visiting Babaji castle, the winter home of the Khan, was one of the highlights of my first deployment to Afghanistan. My time in Afghanistan has shown me the value of Information Operations Intelligence Integration (IOII) throughout all phases of combat operations. How can IOII support winning hearts and minds guiding successful non-lethal operations? My time in the Joint Information Operations Warfare Center (JIOWC), and more specifically facilitating product development in the Human Influence Targeting Cell, has taught me that IOII permits operations and intelligence to

achieve a shared acceptance of the interconnectivity among the physical, information, and cognitive domains of the information environment. The symbiotic relationship between operations and intelligence requires advanced thought processes and an individual with intellectual flexibility in adapting to an ever-changing Complex Adaptive System (CAS) (Hall & Citrebaum 2010, and Sternberg, 2002). This article will discuss the nature of social reality, realizing some general assumptions, and high/low-context cultural patterns IOII can support to win hearts and minds and guide successful non-lethal operations.

Edgar Schein, a world-renowned expert in social psychology, has published over 14 books *Organizational Psychology* (3rd ed., 1980), *Career Dynamics* (1978), *Organizational Culture and Leadership* (1985, 1992, 2004) as well as many others. His study of social groups and the psychology behind individuals in the information environment; i.e., where they work, live, and socialize. His research gives leaders and military officers an edge in the preparation of IO where understanding of socio-cultural dimensions paramount. Social reality refers to those things members of a group regard as matters of consensus that are not externally, empirically testable (Schein, 2010). Social



Coalition Soldier Engaging with Afghan Children

Source: defenseimagery.mil

reality in Afghanistan operates on a different set of norms than in the United States. When individuals hold different assumptions about “reality,” negotiations become difficult thus influencing nations to resort to economic and military power (Schein, 2010). Our training and negotiation approach has changed from the “do as I say” days. American and Afghan leaders have learned to have a respect for the individual, sharing ideas, norms, and beliefs. American and Afghan leaders have learned respect for the individual, sharing ideas, norms, and belief—a new paradigm that has shaped and influenced a new generation in Afghanistan. To win hearts and minds, we must determine a group’s assumptions using systematic research, socio-cultural psychology, and case-study methodology. Afghanistan’s cultures fall into the group assumption of focusing on the past to shape tomorrow (Schein, 2010). They hold family ties and tell stories that date back a thousand years. These stories become lore and legend, making change very difficult. Then Major General David Petraeus, with regard to a need to understand culture, said “knowledge of the cultural ‘terrain’ can be as important as, and sometimes even more important than, knowledge of the geographic terrain.

To understand socio-cultural thought processes, advanced graduate-level analysis and social psychology help establish a baseline (technical, functional, cultural) of the culture in which intelligence practitioners are operating (Hall & Citrebaum, 2010). Afghan society employs a standard known as polychronic time; that is, using time as an approximate standard, a guide, as contrasted to the Western mode of precise adherence to the clock. Middle Eastern countries use

polychronic time to accomplish multiple tasks simultaneously (Schein, 2010). Americans place importance on time as a measure of value and to manage military operations for efficiency and synchronization. Afghans use *Inshallah* (God Willing), as a measure for importance as Afghans feel that if God wills them to be there at 10 am, they will be there because God made it so. When United States personnel make an appointment for a specific time, they better be prompt, because Afghans understand that time is important to Americans. Afghans will be insulted if American leaders are late, but they expect Afghan leaders to be late in respect to *Inshallah*.

Diplomacy becomes problematic if societies hold distinctive assumptions about “reality.” Socio-cultural understanding is integral to looking past the assumptions of a society. Only after days and months of working with village elders and the Afghan people, you begin to see “different types of authority” among Afghan social structure (Schein, 2010).

Intelligence officers who possess advanced graduate-level intelligence-analysis skill sets and who have had multiple deployments are better equipped, as they are already privy to the culture, norms, and typologies (autocratic, paternalistic, consultative or democratic, participative and power sharing, delegative) associated with specific adversaries worldwide. Typology is imperative for the reason that organizational type supersedes many of the macro cultures that exist in the world (Schein, 2010). Large organizations are likely to center most of their time focusing energy that is foreign to remote tribes throughout the world (Morgan, 2006). This is no different in



Afghan Policemen and Soldiers Inspect an Electrical Light Fixture During a Class Session

Source: defenseimagery.mil

the United States Army; the intelligence analyst is subordinate to the organization during combat operations. Soldiers coming into combat for the first time enter with a set of predetermined assumptions and conceptual categories that allow them to discriminate and label most of what they have experienced (Schein, 2010). The more time a first-time soldier spends immersing himself or herself in Afghan culture, the faster the soldier's false assumptions of the Afghan people and their own superiority complex will disappear.

High- and low-context cultural patterns are also present in Afghanistan. In the low-context, "unidirectional culture, events have clear universal meanings; in the high-context, mutual causality culture, events can be understood only in context, meanings can vary, categories can change, and causality cannot be unambiguously established." (Schein, 2010) The Afghan people are high-context people; that is, most of their cultural behaviors are not public. Members of this society are expected to act based on years of interaction.

Adversary political, military, economic, social, and informational infrastructure (PMESII) is extremely difficult to determine when dealing with cultures that are unfamiliar to intelligence analysts. My case that socio-cultural understanding is essential to IOII will eventually allow advanced intelligence personnel to complete PMESII analysis, but only after applying observables (cultural, functional, situational, biometric, and technical). American soldiers who have deployed more than once and have actively engaged the people learning Pashtu and Dari are still low context for the reason that American soldiers are still faced with boundaries that are not in line with the Afghan people's beliefs.

For example, in my first deployment to Afghanistan, I had an Afghan interpreter who presented himself as pro-Afghanistan wanting to rid his country of Taliban oppression. He taught me Pashtu and introduced me to his culture. This added to my credibility during meetings with village elders. I reciprocated the teaching by sharing with my interpreter American military values, without ever discussing religion, which was prohibited by command. We later realized, however, that he had only played the part of pro-Afghanistan for months, providing the enemy with tactics, techniques, and procedures (TTPs). The lesson learned was that no matter how hard you try to understand Afghan view of themselves and us, the reality is much more complex and the loyalties can be shifting and adjustable even among Afghans who are helping the coalition.

Active listening will get you far in Afghan culture. Village elders love to talk and tell their war stories from their time fighting the Soviets. Cross-cultural communication strategies suggest that a local interpreter can aid you to develop a bond with the local populace. I am still a fan of using local interpreters to help the leader in bringing down barriers Afghan people may have when they see soldiers with weapons. As a result of the Taliban interpreter providing the adversary with TTPs, I changed many aspects about our operation, making our teams more efficient and less dependent on Afghan help to enhance operational security. I devoted myself to learning more about the Afghan culture in

order to remove any misconceptions I might have been using at the time.

As leaders, we must continue to learn from our victories and defeats and trust our instincts. By coming to terms with the true nature of social reality, grasping group assumptions, and recognizing high/low context cultural patterns, IOII can support winning hearts and minds guiding successful non-lethal operations. 🌐

References:

1. Hall, Wayne. M. (2010). *Intelligence Analysis: How to Think in Complex Environments*. Santa Barbara: ABC-CLIO, LLC., page 205-2173.
2. Merriam Webster. (1999). *Merriam Webster's Collegiate Dictionary: Tenth Edition*. Springfield: Merriam-Webster, Inc.
3. Scullard, Howard. H. (1970). *Scipio Africanus: Soldier and Politician*. New York: Cornell University.



US Army Captain Gustavo A. Molina is assigned to the Joint Information Operations Warfare Center in San Antonio Texas. He works as the intelligence branch chief of the human factors intelligence branch of the operations directorate. His branch focuses on human factors intelligence and IOII and intelligence support to information-related activities.



Afghan Man Waits for Ribbon Cutting And Graduation Ceremony at Boys High School

Source: defenseimagery.mil

Face and Information Operations

By

Major Douglas Wilber, US Army Retired

Editor's Note: The concept of "face" is extremely important in many societies. Western and developed societies have lost some of the importance of "face" in their transition to the importance of the individual, but in many parts of Asia and the Islamic world "Face" is a critical component of society. This makes it a very important consideration in IO.

A recent video of a US Army Police Advisor yelling at Iraqi policemen for cowardice and treachery became an overnight YouTube sensation.¹ While the soldier probably had good reasons for being angry, he certainly caused a variety of problems for the coalition forces. One problem in particular is that these officers and their community 'lost face' in a country where honor is social capital. He also caused the coalition to lose face with the people they needed support from. The soldier probably never realized the consequences of his actions because he failed to understand how important 'face,' or honor was in Iraq. While conventional wisdom advises that, you should praise in public and scold in private, there is little indoctrination or training that discusses the role of face in intercultural communications.

Most Americans would probably assume that the concept of face involves avoiding embarrassment or establishing a good reputation. They might also assume that face is somewhat more important in Asian than in Western cultures; however, face is more important than most people think. Face is an essential element in effective inter-cultural communication and failure to act accordingly can doom an intercultural relationship. For deployed military personnel, respect of face can mean the difference between provoking violent conflict and gaining someone's cooperation. Therefore, it is vital that military personnel and their civilian counterparts know how to respect and enhance the face of their engagement partners.

What is Face?

Face is essentially a projected image of one's self or group in a relational situation. In other words, face is how you want a specific group or person to perceive you. Failure to maintain this image can result in face loss depending upon the people and context involved. Face is context and culturally dependent as one projects different types of face with different people or groups.² People can create a "Dr. Jeckle and Mr. Hyde" type dichotomy by creating different personalities for different audiences. For example, a drill sergeant's face among recruits is different from what he would project with his friends and neighbors. Tripping and falling while on a march might cause him to lose face with recruits but not with his friends.

Face-work is the process of managing one's image by following the unwritten rules of social interaction within a given culture.³ Judges have to maintain the image of being upstanding and moral members of society in order to justify the power they exert over other people. If a judge were caught on tape being drunk and disorderly, he would lose face, while a vagrant would not lose it because he is often expected to be drunk, and to act that way. Thus, to engage in face-work, you must understand the rules of interaction within a society. For instance, the rules of interaction within military culture are so different from the

rules within civilian society that basic training is required to teach civilians to be a soldier. Thus, problems arise when a person applies rules appropriate for one culture in a relationship with a person from another culture.

There are three types of face orientation that all people and groups practice: self, other or group, and mutual. Self-face belongs to a unique individual, whereas other-face belongs to another person or group. Mutual-face is shared between oneself and others; although, these two do not have to belong to the same group. You can engage in face-work strategies that focus on enhancing your self-face, giving face to others or enhancing mutual face.⁴ In reality, all people engage in all three types of face-work, depending on the context of the situation. A person who is highly concerned with self-face at work may freely give other-face to their friend during social situations and engage in mutual-face-work with their bowling club. The context of the situation and the interaction rules at play will have a significant consequence upon what orientation one employs.

Face-work orientation is affected by how collectivist or individualistic a culture is. Individualistic cultures place more value on self-face since their individual identity is more salient; therefore, people in these cultures will engage in face-work to preserve their self-identity. If one's self-face is strongly integrated with another's, as a parent-child relationship would entail, then protection of another's face is as important as protecting self-face. Collectivist cultures have the opposite tendency and are more concerned with protection of the group's image. They mostly engage in other- and mutual-face-work since their identity within a group is more significant; however, these individuals are still concerned with their own self-image, especially within the group.⁵

In a work situation, an individualist will want to project an image of individual excellence that leads the boss to think highly of them. They are less likely to try and give face to their peers, and are unlikely to take the blame for failure in order to preserve group face. A collectivist will more often 'take one for the team' by sacrificing their self-face to protect the group's identity. They are also more concerned with giving face to others in the group, especially their superiors. Thus, in a collectivist culture, threatening group face will provoke more resistance than threatening an individual's identity. The exception would be an iconic individual like the Prophet Mohammed whose identity is thoroughly infused within the Muslim group identity. What made the yelling incident so dangerous is that the soldier threatened the group identity of the Iraqi police and parts of their social network. These Iraqis would be very likely to sacrifice themselves in order to preserve the group's face.

Collectivist cultures value face and face-work more than individualistic cultures. They will expend more resources in order to maintain face and will react aggressively when it is threatened. People in collectivist societies are more interdependent with their in-group members than in individualist societies. Extensive interdependence requires that the groups establish strict rules for personal conduct in order to ensure group cohesion that prevents face loss and conflict.

Every person has a role and place in the group's hierarchy, and adhering to this role preserves the face of others. This exists within military culture where teams must subvert their individual needs to those of the group in order for that team to fight effectively.⁶

Collectivists are concerned with maintaining the harmony and face of their in-groups, but not with out-groups. Research shows that collectivists make stricter differentiations between in and out groups than individualists.⁷ In a business transaction an individualist will generally have little concern about working with someone from an out-group, while a collectivist would have a greater reluctance. This tendency can intensify a conflict in collectivist societies who see an attack on the out-group as gaining positive face for them. This reality has face-work implications for military personnel who have to cope with it, but that will be discussed later.

Face-Work and Conflict

Threatening the face of another person or group will almost certainly cause some form of conflict; however, these conflicts can either be prevented or mitigated through good face-work. Since face-work is essentially a communication activity, the communication styles and methods employed have a profound impact upon whether you give face or threaten it. The greater the difference between two cultures, and the more probable a conflict generating miscommunication becomes. This is enhanced in collectivist cultures when the offender is a member of an out-group. Thus, a US military overseas operation is fraught with the potential for conflict over face. Understanding whether a culture is high or low context provides an essential starting point for conflict resolution face-work.

America and all other individualistic societies are low context cultures (LCC) in that their communication styles are primarily verbal, direct, and assertive. Ideally messages stand-alone and do not require any additional visual aides to understand. LCC communication relies less upon factors within the environment, or nuance, of the relationship between the parties to deliver a message. Due to a lower level of inter-dependence, maintaining harmony in relationships is less important. Individualists also have an ability to separate the issues in a topical conflict from the relationship in general. Thus, LCC are task oriented, and have a short-term perspective of time which is why Americans prefer to get to the bottom line quickly.⁸ In the U.S., if your zipper is down someone will usually tell you without concern that it might embarrass you in the short-term. Thus, the soldier who berated his Iraqi advisees was communicating in a low context manner that was essentially normal for him.

High context cultures (HCC) are usually also collectivist societies like those in the Middle East, Asia, and Russia. They rely less upon verbal communication, preferring more subtle and indirect methods like non-verbal cues. HCC uses communication to preserve group face and maintain harmony by compelling the communicator to follow strict rules of interaction. They have a harder time separating conflict about a specific topic from the relationship in general. Tactfulness is very important, and they are very concerned with ensuring that a message is appropriate within a specific context. If your zipper is down in Asia, they may not tell you directly, but rather signal it through non-verbal language in order to avoid embarrassing you. In HCC, preservation of the long-term relationship is more important than delivering the message.⁹

Poor intercultural communication causes conflict initiating face loss between collectivist HCC and individualist LCC parties. LCC members, especially military personnel, will often prefer

the dominating conflict style, which manifests itself in blunt and assertive talk. These assertive and direct messages threaten a collectivist's face because they are so contrary to their rules of social interaction. Dominating strategies are often avoided in HCC because they are threatening to the relationship. Direct and overt communication that lacks tactfulness can shock an HCC member, especially if he is in the presence of his primary group.¹⁰ Threatening the group's face obliges its members to sacrifice their own well-being to preserve or restore group face.

Conflict can also result from the conflict styles HCC and LCC societies use to manage face-work. People in HCC prefer to use avoidance strategies to manage conflict since they prefer to maintain harmony and preserve relationships. The use of ambiguous and subtle communication helps to avoid conflict and preserve face. People in LCC would find this approach to be offensive since they can perceive that they are being ignored, which causes self-face loss. They might react by being more direct and aggressive in their communication style. This was a common problem in Vietnam between American advisors who frequently complained that their Vietnamese counterparts were ignoring and avoiding them. The Vietnamese probably just wanted to avoid conflict that could jeopardize their face with superiors.

Face-Work Strategies

Two main super-strategies exist for maintaining and enhancing the face of a person or a group. The first super-strategy is prevention, which is communication behavior designed to preclude face-loss, or cover face vulnerabilities. The second super-strategy is restorative face-work, and is designed to repair lost face after an incident. These two strategies are often done in conjunction with each other, and prevention is done before, during and after a face loss incident.¹¹ These strategies manifest themselves in a number of communication behaviors determined by culture and the context of the situation. A problem can arise when parties in an interaction misunderstand the purpose of these face-work behaviors.

Preventative face-loss strategies are proactive, dynamic, and used continuously. Collectivist cultures engage in more prevention behaviors than individualists do because they want to preserve harmony and avoid conflict. Many social interaction rituals are designed to serve a preventative purpose. Most military personnel who have interacted with Arabs have wondered why they always begin and end a meeting with small talk. Extensive research has shown that they follow this pattern in order to establish the party's role and hierarchy in the relationship. It is a preventative face-work strategy known as credentialing where a person or group establishes their bona fides before the interaction.¹² When analyzing and interpreting seemingly strange behaviors from your interaction partner, it would be prudent to identify if they are employing a prevention strategy.

Preventative strategy often includes a suspended judgment appeal where you ask someone to hear and consider your argument before you make it. If you are going to make a claim that is likely to provoke an immediate negative response from an audience because you appear to be assaulting their beliefs, you can initiate by making a suspension statement. For instance, if you want to stop a foreign counterpart from abusing a detainee who just hurt one of their troops, you can ask them to hear you out so they can consider the advantages of not beating him. Another strategy is a pre-disclosure statement that helps the audience to bond or identify with you before you make a critical statement.¹³ Before you want the foreign troops you are advising to engage in an after-action review, you may want to

let them see you do it with your team first. Since you subject yourself to this face-threatening act, it eliminates the impression that you are just trying to be judgmental with them.

The third strategy is a pre-apology to lower expectations from the other party, so there is less face loss in the event of failure. To the average American servicemen, hearing a pre-apology from a military or civilian counterpart may seem defeatist or create the impression that they intend to fail. In many ways, the statement “Insha’Allah” which means “God willing,” in Arabic, is a type of pre-apology. The disclaimer handicaps the speaker by his statement that he cannot do something. A tribal sheikh who wants to avoid cooperating with you in providing security for an area can create the impression that he is poorer or less influential than he really is. Another example would be if your police counterpart states that he cannot go on a dangerous operation with you because he doesn’t have gas for his trucks.

Face-restoration strategies are designed to repair face loss after it occurs and can be used to repair a relationship or restore an image of strength. Individualists engage in more face restoring behaviors than collectivists since they engage in fewer prevention behaviors. The type of strategy used depends upon the relationship. Aggressive strategies are used if the relationship is not important; however, when the relationship is important, one would use more self-deprecating unassertive strategies. In collectivist cultures the key to the type of restorative strategies preferred is whether the other party is part of the in-group or out-group.¹⁴ Restoring face among in-groups requires an unassertive strategy, while out-groups would often dictate an assertive strategy.

The first face-restoration strategy is direct aggression, in which you attack the person or group who caused the face loss. In a tribal conflict, the blood feud is often a form of this, where a ‘tit for tat’ exchange of violence is necessary to preserve face. Yelling and threatening are direct aggression gestures short of violence, which are also tactics, used to restore face. The second face-restoration strategy is passive aggressiveness, where you might deny the incident or act confused in order to mitigate face loss. This is a good strategy for weaker parties to resist

stronger ones when strategies that are more overt would not be acceptable. If you cause a local government official to lose face, he might fail to implement actions that are needed for a civil affairs project. Plain avoidance is also an option that can often be interpreted as aggressive since it seeks to avoid any productive resolution of the problem.¹⁵ Both of these strategies are best reserved for use against out-groups, especially when the relationship is not important.

The third face-restoration strategy is making an excuse that minimizes personal or group responsibility for the face-loss incident. Excuses can blame the problem on dispositional attributions that ascribe the cause of an event to the individual. An excuse can also make situational attributions that lay the blame on external factors beyond an individual’s control. Collectivists are more likely to use dispositional accounts to describe failure in order to save group face. Individualists are more likely to use situational attributions to avoid self-face loss. Physical remediation is a restorative strategy, and is where you take immediate action to help and correct the situation. If one accidentally kills or injures someone at your checkpoint who was not a threat to you, making a ‘solutia payment’ is a physical remediation. The final strategy is using apologies that alleviate guilt, or shame, when the offending party is willing to admit their responsibility.¹⁶

Implications for Information Operations

The reality of face and face-work has profound implications for the planning and execution of information operations (IO). Every culture is unique and has different rules of social interaction that guide the use of face-work. An IO practitioner must try to understand as many of these rules as possible. There is no substitute for doing the research and relying upon the advice of legitimate cultural experts. In communication with members of high context cultures, you should acknowledge that, as a foreigner in their country, you do not fully understand their culture and do not mean to offend them.

The IO practitioner should seek to integrate face-prevention strategies into soldier and leader engagements with the indigenous population of the host country. These interactions present the



Afghan National Army Public Affairs Specialist in Photography Class

Source: defenseimagery.mil

most opportune and the most dangerous communication situations. Mutual-face prevention activities are ideal since you usually want to build a relationship. Taking the time to drink tea and chat with an Arab in their home with your body armor off gives them face since you are demonstrating trust that they protect their guests. They will be obliged to reciprocate and engage in face-giving behaviors that may benefit your mission. Accounting for and accepting your partners' face-prevention strategies are essential.

Sacrificing some of your self-face in order to give it to your partner is a viable and potentially a high-payoff situation. Shifting the blame from a potential incident like a risky mission from your partner to yourself is an innovative strategy. Arranging to give them the credit for success multiplies the potential effect of this strategy. Saving face matters less to Americans, we can take a small hit to our pride much easier than our partners can. Sacrificing our face for the benefit of the mission can pay off through the creation of strong relationships. However, you have to risk assessing this face sacrifice so you are not going to lose the wrong kind of face. For instance, you can't risk your image as a protector of human rights to cover for your partner's abuse of them.

Furthermore, the IO practitioner needs to recognize the salience of group face in collectivist cultures. Assaulting a group's face is going to have serious consequences and can create serious resistance. Thus, when you need to attack someone in a group, it is wise to isolate them from the group. One might want to simultaneously assuage the group's face in order to mitigate the chances of a negative reaction.

In general, it is always prudent to give face to others as much as possible. These behaviors can be used to influence indigenous leaders to undertake actions that need to be performed. Publicly praising a leader in front of his people gives both self and group positive face. Denying aid to certain officials is a face-threatening activity and should be done prudently with the risk knowingly assessed. Furthermore, criticizing or being openly intrusive in their operations threatens their negative face. Discover what methods of inspection and correction are considered to be appropriate in their culture and seek to emulate them to the best extent possible.

Conclusion

The reality of face requires that military personnel and their civilian counterparts acknowledge the impact it can have upon operations. All people have a self-image, as well as the groups they belong to, and all engage in some form of face-work to control this self-image. In collectivist cultures, face is more important and their group identity is more salient. Because we predominantly operate within collectivist cultures, face is a crucial aspect of human terrain. Face is both a liability and an asset depending upon how you manage it. If you threaten someone's face, you create a liability since they will certainly resist you in some way. If you protect or enhance the face of another, you can win their compliance or even their allegiance. The worst thing deployed military personnel can do is to ignore the reality of face, which will certainly cause conflict.

Since face-work is a communication behavior, its planning and management will often fall within the realm of IO. Face will be most critical during leader and soldier engagements with the indigenous population. Face and its application must be included into the comprehensive pre-deployment, and during deployment training program. Face must be managed throughout the course of the relationship and the deployment. The engagement staff officer must track face-work and adjust

engagement tactics to achieve the most optimal effect possible. Additionally, Military Information Support Operations and Public Affairs activities must be managed to account for face-work. Thus, the IO practitioner must work hard to capitalize on this potential asset while avoiding face-threatening acts that can make unnecessary enemies. 

Endnotes:

1. *The Video Clip of the U.S. Army Soldier berating a group of Iraqi Policemen* was retrieved on 5 December 2011 from, <http://www.youtube.com/watch?v=JGbQB18K1Co>.
2. Gudykunst, William B, and Seichi Morisaki. "Face in Japan and in the United States", in *The Challenge of Facework: Cross Cultural and Interpersonal Issues*, edited by Stella Ting-Toomey, 47-93. Albany: State University of New York Press, 1994.
3. Ting-Toomey, Stella. "Intercultural Conflict Styles: Face Negotiation Theory" in *Theories in Intercultural Communication*, edited by William Gudykunst, 213-233. Fullerton: California State University, 1988.
4. Ting-Toomey, Stella. "The Matrix of Face: An updated face negotiation theory", in *Theorizing about intercultural communication*, edited by William Gudykunst, 71-92. Thousand Oaks CA: Sage, 2004.
5. Ting-Toomey, Stella. "Translating Conflict Face-Negotiation Theory into Practice", in *Handbook of Intercultural Training*, 3rd edition, edited by Dan Landis, Janet M. Bennett, and Milton J. Bennett. pp. 217-248. Thousand Oaks, CA: Sage. 2004.
6. Oetzel, John, and Stella Ting-Toomey. "Face Concerns in Interpersonal Conflict: A Cross-Cultural Empirical Test of the Face Negotiation Theory," *Communication Research* 30 (December 2003): 599-624.
7. Ting-Toomey, *Intercultural Conflict Styles: Face Negotiation Theory*, 47-93.
8. Ting-Toomey, *Translating Conflict Face-Negotiation Theory into Practice*, 217-248.
9. Ting-Toomey, *Translating Conflict Face-Negotiation Theory into Practice*, 217-248.
10. Chang, Hui-Ching, and Richard G. Holt. "A Chinese Perspective on Face as Inter-Relational Concern", in *The Challenge of Facework: Cross Cultural and Interpersonal Issues*, edited by Stella Ting-Toomey, 95-132. Albany: State University of New York Press, 1994.
11. Ting-Toomey, *The Matrix of Face: An updated face negotiation theory*, 71-92.
12. Scollon, Ron, and Suzie Wong Scollon. "Face Parameters in East-West Discourse", in *The Challenge of Facework: Cross Cultural and Interpersonal Issues*, edited by Stella Ting-Toomey, 231-267. Albany: State University of New York Press, 1994.
13. Ting-Toomey, *The Matrix of Face: An updated face negotiation theory*, 71-92.
14. Ting-Toomey, *Translating Conflict Face-Negotiation Theory into Practice*, 217-248.
15. Edelman, Robert J. "Embarrassment and Blushing: Factors Influencing Face-Saving Strategies", in *The Challenge of Facework: Cross Cultural and Interpersonal Issues*, edited by Stella Ting-Toomey, 231-267. Albany: State University of New York Press, 1994.
16. Edelman, Robert J. "Embarrassment and Blushing: Factors Influencing Face-Saving Strategies", 231-267.



MAJ Douglas S. Wilbur, USA RET served an FA 30 Information Operations Officer. He deployed three times to Iraq and once to Kosovo. He holds a B.A. and an M.A. in International Relations from St. Mary's University. Douglas currently works as a public relations and public policy manager for South Texas Mother's Against Drunk Driving. He is working towards a Ph.D. in communication, where he intends to specialize in international and intercultural communication.

IO SPHERE

GENERAL CALL FOR ARTICLES

Become a Contributor

IO Sphere welcomes your articles, papers, and commentaries regarding all aspects of full-spectrum Information Operations and Information-Related activities and capabilities, as well as IO intelligence integration. Articles or book reviews should be 600-3000 words, preferably with an operational, training, or similar focus as related to IO. Contact the editor for submission guidelines at jiowc.iosphere@us.af.mil.

Published Quarterly in Digital Journal Format Submission Deadlines

- 15 February - First Issue of Year
- 15 May - Second Issue of Year
- 15 August - Third Issue of Year
- 15 November - Final Issue of Year

INFORMATION: If you or your organization would like a free information and updates on *IO Sphere*, write to the editor at jiowc.iosphere@us.af.mil. Please include your name, organization, office or division, official mailing address with 9-digit zip code and number of individuals in your organization. For more information, contact the *IO Sphere* editor at (210) 977-5227 or DSN 969-5227.

Submission Guidelines

Please submit your contribution in Microsoft Word format, version 6.0 or higher, double-spaced in 10-point, Times New Roman font. Place graphs, photographs, and/or charts in separate attachments, not in the body of the paper. Insert a note describing object placement in the body of the paper. Example, "Place attachment one here." All charts/graphs/photographs should be at least 200 DPI resolution and in TIFF or JPEG format. Also, you may submit a high-quality hard copy of graphics for scanning.

For additional submission details on the *IO Sphere*, contact the editor.

Email all unclassified submissions to the editor at jiowc.iosphere@us.af.mil. Point of contact is the *IO Sphere* Editor, Mr. Henry K. Howerton at 210-977-5227 or DSN 969-5227. *IO Sphere* is published at the unclassified level only. Also, all items should be security screened, and released by author's parent command/agency/organization/company prior to submission. Please include a letter or email documenting these actions.

Currently Seeking Submissions on all Information-Related Activities Including Electronic Warfare, Public Affairs, Communication Strategy, Military Information Support Operations, IO Education and Training, IO Intelligence Integration, IO Assessment and IO Support to Public Diplomacy.



IO SPHERE: INFORMATION REQUEST FORM

Command/Organization: _____

Group/Dept./Division Name: _____

Attention Line: _____

Number & Street Address or Box: _____

City, State/Province: _____

ZIP +4 or Postal Code _____

POC: _____ Phone #: _____

E-mail: _____ **FOLD UP HERE** _____

How many people there involved in IO? _____

How did you get this journal? _____

Which article(s) did you find most useful? _____

Which article(s) did you find least useful? _____

What would you like to see in future editions or on our website? _____

Information on SIPRNet at: <http://www.intelink.sgov.gov/sites/jiowc/products/advocacy>

Under "lists" click "IO Sphere Subscription"

On Internet Via APAN at: <https://community.apan.org/ioc/p/customlists.aspx>

FAX TO: (210) 977-4654 (DSN 969) or Email: jiowc.iosphere@us.af.mil

FOLD BACK HERE _____

OFFICIAL BUSINESS

PLACE
POSTAGE
HERE

**JOINT INFORMATION OPERATIONS WARFARE CENTER
ATTN: IO SPHERE EDITOR / J55 Advocacy Branch
2 HALL BLVD STE 217
SAN ANTONIO TX 78243-7074**

September 2012



"Support the Joint Staff in improving DoD ability to meet combatant command information-related requirements, improve development of information-related capabilities, and ensure operational integration and coherence across combatant commands and other DoD activities."

Mission of The Joint Information Operations Warfare Center (JIOWC)
CJCSI 5125.01. 1 September 2011



JOINT INFORMATION OPERATIONS WARFARE CENTER
2 HALL BLVD STE 217
SAN ANTONIO TX 78243-7074