

December 2011

I O SPHERE

The Professional Journal of Joint Information Operations

IN THIS ISSUE

Information Operations in the Age of
Shrinking Budgets: Crisis or Opportunity?
Brigadier General John N.T. Shanahan,
US Air Force pg2

World Wide IO Conference 2011 pg3

Information Operations: Decentralized
Support of Battle Command
Major Jay H. Anson, US Army pg4

The Next Decade and Beyond: Foundational
Force Development for a New IO
Mr. Jonathan Drummond pg10

The Value of Graduate Level Education in
Information Operations
Captain Roy Petty &
Captain Stephanie Helm, US Navy pg20

Trouble on the Airwaves: Countering Radio
Propaganda in Information Operations
Major Lynn Berg, US Air Force pg25

Protecting Sensitive Emails
Mr. Aaron DeVaughn pg33

War Control and Electronic "Shi"-China's
Electronic Reconnaissance Goals
Mr. Timothy Thomas pg35

The IO Force



Joint Information Operations Warfare Center





IO SPHERE

FEATURE ITEMS and ARTICLES

Information Operations in the Age of Shrinking Budgets: Crisis or Opportunity? John N.T. Shanahan, Brigadier General US Air Force.....	2
World Wide IO Conference 2011	3
Information Operations: Decentralized Support of Battle Command Jay H. Anson, Major US Army.....	4
The Next Decade and Beyond: Foundational Force Development for a New IO Mr. Jonathan Drummond.....	10
The Value of Graduate Level Education in Information Operations Roy Petty, Captain US Navy and Stephanie Helm, Captain US Navy (Retired).....	20
Trouble on the Airwaves: Countering Radio Propaganda in Information Operations Lynn Berg, Major US Air Force (Retired).....	25
Protecting Sensitive Emails Mr. Aaron DeVaughn, Department of the Air Force Civilian.....	33
War Control and Electronic "Shi"-China's Electronic Reconnaissance Goals Mr. Timothy Thomas, Department of the Army Civilian.....	35



Credit and thanks to our graphics and layout editors Ms. Gloria Vasquez and Mr. John Reyna of the US Air Force ISR Agency, and copy editor Mr. Bruce Judisch, MeriTec Inc. and 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 cover represents the various aspects of operational IO. The back cover represents IO professionals, as well as, the mission of the Joint Information Operations Warfare Center.

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 rotation of the US military service colors and the color purple to symbolize the joint nature of Information Operations.

Cut Along Line

Ms. Sandra Vasile
JIOWC J5, Executive Editor

Mr. Henry (Keith) Howerton
Editor and Layout Design
Webhead Inc

Mr. Bruce Judisch, MeriTec Inc, Copy Editor

IO Sphere Staff

Ms. Gloria Vasquez and Mr. John Reyna
Graphics Editor and Layout Design

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 SiperNet at: <https://www.jiowc.smil.mil/publications/IOSphere/Default.aspx>

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

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



MISO in Afghanistan

US Army soldier gives an Afghan man a recruiting poster from the local monthly newsletter "Freedom's Voice" in Marjah, Afghanistan.



GENERAL SUBMISSION GUIDELINES:

IO Sphere welcomes submissions of articles regarding full-spectrum IO, including all information-related capabilities. *IO Sphere* also welcomes book reviews and editorial commentary on IO and defense-related topics. Submission deadlines are flexible and it is best to send a submission when it is ready. The *IO Sphere* staff will work to get it included in a future issue.

TEXT - Microsoft Word.

CHARTS/GRAPHS - TIFF, GIF, JPG format or powerpoint with one graph or chart on each page.

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
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 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 J55 Advocacy Office of the Joint Information Operations Warfare Center under the direction of the US DOD Joint Staff J39/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.**

Information Operations in an Age of Shrinking Budgets: Crisis or Opportunity?

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

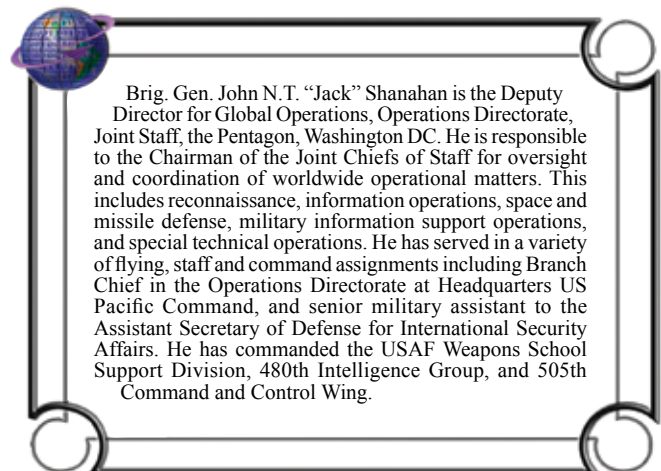
Within the past year, we have seen some of the most far-reaching changes in a decade across the field of Information Operations (IO). Whether codifying a new definition of IO, realigning functional areas, or restructuring organizations, the sweeping changes are significantly altering the breadth and depth of IO. There were myriad reasons for the ground swell that led to this flurry of activity, to include confusion resulting from different and often competing definitions and practical applications of IO, Strategic Communication (SC), and Public Affairs (PA); unwanted attention resulting from field operations that went awry; renewed emphasis by the Combatant Commanders on the importance of IO; and an overdue focus on regaining efficiencies. The progress has been impressive, but we have a long way to go to institutionalize the changes. We are working closely with OSD, the Services, and the combatant commands to outline the necessary next steps. Yet as we do so, we are also facing what promises to be the most challenging fiscal environment DOD has faced in a quarter century. There is no question that information-related capabilities (IRC) will absorb substantial cuts. Is this a crisis or an opportunity? As I see it, the answer is glaringly obvious: it's an opportunity we literally cannot afford to pass up.

A phrase attributed to Winston Churchill during the dark early days of World War II immediately comes to mind in the



current fiscal environment: “Gentlemen, we have run out of money. It’s time to think.” Our priority is to provide the best possible IO support across the spectrum of operations, from Phase 0 through high-end combat and post-conflict stability and reconstruction operations. We need your help in taking a bold approach to enhance IRCs. This will take many forms, from developing and strengthening IO intelligence analysis and integration, to fully integrating IO into operational planning (to include use of special technical operations), to ensuring IRCs are continuously evaluated and modified during mission execution, to devising new methods to tackle the age-old challenge of IO assessment. Most importantly, we need you to take the axe to efforts that do not advance the commander’s objectives or that are unnecessarily duplicative. As the previous Secretary of Defense emphasized in his memorandum earlier this year, IO is about the integration of IRCs to achieve desired effects. It is not about ownership of individual capabilities. The looming fiscal environment will simply not allow us to focus on individual platforms or niche capabilities; we must all work together to integrate what already exists and to develop new and innovative ways to employ IRCs.

For instance, the exponential growth of cyberspace operations is one key area that opens up remarkable new possibilities in IO while not demanding a commensurate increase in applied resources. When it comes to IO, cyberspace must never be an end to itself; instead, it offers another means to integrate IRCs to achieve the desired effects. Effects developed by people for people...we cannot lose sight of the challenge of trying to influence an adversary or potential adversary who is complex, adaptive, and a sentient human being. In essence, we end up with cyber-enabled IO or cyber-enabled MISO, not cyber for cyber’s sake. What we need from you are the good ideas that take advantage of cyberspace without sowing the seeds of another stovepipe capability. At the same time, we must adapt extant government and commercial off-the-shelf solutions and invest in qualitative advances in human capital to grow a new generation who are as comfortable integrating a wide range of IRCs as they are hammering out a 140-character Tweet. And while we must recruit, develop, and promote our IO subject matter experts—who will always represent the core cadre of IO professionals every commander must have nearby—we also need everyone else to become reasonably proficient in integrating kinetic and non-kinetic, and lethal and non-lethal IRCs. The “super-empowered individual” enabled by the explosive growth of cyber capabilities can just as easily become a super-empowered IO-er without too much formal IO training. You just need to keep him or her pointed in the right direction.



Brig. 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, and 505th Command and Control Wing.

Crisis, what crisis? We have a unique opportunity in front of us to continue to make impressive across-the-board gains in IO. When you come up with those new, innovative ideas about how to better employ IRCs, we will work closely with you to figure out how to turn ideas into fielded capabilities or to develop the appropriate programmatic and/or acquisition-related actions. We have made a lot of headway, but we cannot afford to slow down or bemoan the fiscal environment looming before us. We need a concerted, sustained effort by the entire IO force to adapt, to innovate, and to convince your commanders how IRCs are a force multiplier that open up new possibilities across the entire spectrum of conflict. In other words, when other high-end capabilities become increasingly scarce due to fiscal pressures, IO may offer one of the best alternatives to generate the desired effects. We are here to help. Let me know what we can do for you. ●

Brig Gen Shanahan

Worldwide Information Operations Conference 2011 “Information Operations as a Traditional Military Activity”

Chantilly, VA-(September 28-29, 2011) The 2011 Worldwide Information Operations Conference (WWIO) held in Chantilly Virginia punctuated a critical juncture in the future of IO.

The Joint Staff Deputy Director for Global Operations (DDGO) and Joint Staff J-39 host the annual event on behalf of the Department of Defense and allied IO community. This year’s conference was the first WWIO to be hosted by the new DDGO and J-39, US Air Force Brigadier General John N.T. Shanahan. In his welcome letter, General Shanahan set the tone for the conference. He wrote, “This year’s conference brings together a myriad of IO professionals from around the world to meet and discuss a common goal—integrating information-related capability from across the Department of Defense, the US Government, and partner nations to produce synergistic effects within the information environment to achieve a desired end state. Our speakers, panel discussions, and briefings are designed to be thought-provoking and generate a productive dialogue....this gathering is an excellent opportunity to make new contacts and expand your horizons in the dynamic world of Information Operations.”

The 2011 conference proved informative and eventful. Special guest speakers included Mr. Michael D. Lumpkin, who serves as Principal Deputy Assistant Secretary of Defense for Special Operations and Low Intensity Conflict and Independent Capabilities (SO/LIC&IC), and Major General Thomas K. Andersen, Vice Commander of the Air University at Maxwell Air Force Base, Alabama.

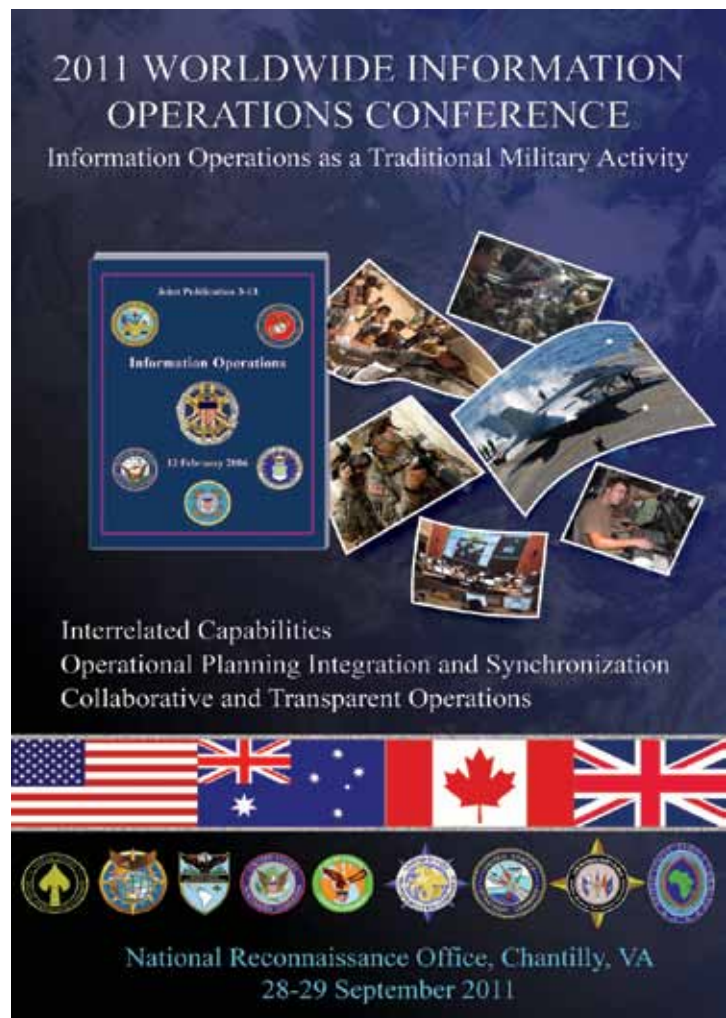
In addition to the special guest speakers, the combatant command IO directorates and each of the service IO organizations presented briefings highlighting efforts and initiatives in their respective areas of responsibility.

Mr. Austin Branch from the Office of the Secretary of Defense for Policy led several panel sessions that included senior-level discussions on the state of IO, one in particular focusing on the theme of the conference of IO as a traditional military activity. Additional presentations spanned a wide variety of topics, to include cross-cultural communications, the Joint IO Range, moderate Islam,

strategic communication and security cooperation, IO force development, and IO intelligence community of action update. Allied presentations from the United Kingdom, Canada, and Australia on IO focused on IO efforts in their respective countries.

The 2011 WWIO conference clarified and provided detail on the new definition of IO contained in the US Secretary of Defense memorandum titled “Strategic Communication and Information Operations in the DOD,” dated January 25, 2011, which reads, “the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.”

According to the conference organizers, another major theme of the gathering was to refocus from the traditional core functions of IO to integrating “information-related capabilities.” This represents a significant redirection in the way the IO line of operation and the forces that execute it will be organized, trained and provisioned for the future. Additionally, the dynamic pace and changing demands of the operational community IO supports, paired with increasingly severe DOD-wide funding constraints, require such a refocus. And although the challenges in restructuring to meet these operational needs in a fiscally austere environment are considerable, they harbor new opportunities for the IO community to impact operations in broader and more meaningful ways. ●



Information Operations: Decentralized Support of Battle Command

By

Major Jay H. Anson, US Army

Editor's Note: Major Anson first published this essay as part of the academic requirements for the US Army Command and General Staff Officer Course at Fort Leavenworth Kansas in 2010. His experience in the war on terrorism and other operations make his observations on IO battle command relevant. At the time this article was drafted Psychological Operations had not changed to Military Information Support Operations. The term was editorially changed when possible to MISO.

In just the first decade of the 21st century, the world has seen the emergence of newer and more innovative information technologies, as well as increasingly inventive uses of these systems. Information operations (IO) have developed into a universal mainstay in all aspects of public and private life; for example, to shape public opinion during political campaigns, augment commerce through online shopping, share information and remain connected with friends and colleagues using social networking sites, and provide instantaneous statuses and feedback to the world via microblogging services. The United States Army has moved swiftly to procure the latest information technology and revise its IO doctrine, adapting both to the current force structure, operating environment, and command and control (C2) enablers to maintain information superiority on and off the battlefield. Information Operations that influence and inform populations at home and abroad, protect our systems, people, and information, and exploit,

influence, and disrupt our enemies' will and ability to fight are critical to success at the strategic, operational, and tactical levels of war. Current Army doctrine defines in detail five essential IO tasks paramount to achieving and maintaining information superiority during full spectrum operations. Commanders and staff at the operational level implement information engagement, C2 warfare, information protection, operations security (OPSEC), and military deception to the greatest degree possible.¹ Units have tried a variety of techniques at the operational level to develop a standardized, practical and effective way to carry out IO tasks and effectively integrate them into "battle command" (BC). The best way to accomplish this is to emphasize organizational staff strengths and align the IO tasks accordingly to gain the desired effects. This also requires unity of effort and clear roles and responsibilities for each information task throughout planning and execution. Putting IO into action should require no significant modification to existing task organization or new staffing requirements. The staff organization at the Service component headquarters should be integrated into a joint task force construct without difficulty. By 2025, the IO structure described in this paper should be standardized across Army formations.

Battle Command requires more than just understanding and visualizing the operational environment. The overall objective of IO in relation to the art and science of BC, according to Army doctrine, is to "impose the commander's will on a hostile, thinking, and adaptive enemy."² Commanders, through their



US Soldiers Conduct Battle Command Drills in Anti-IED Training Lane in Iraq

Source: defenseimagery.mil

JOINT INFORMATION OPERATIONS PLANNERS COURSE



Joint Forces Staff College



Only DOD Certification Course for Joint IO Planner's

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 Core, Supporting and
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



staffs, therefore must effectively employ IO capabilities through meticulous coordination and synchronization, cross-leveling and sharing information and resources while keeping everyone on the same message. The implementation techniques, standard operating procedures (SOP), and assignment of IO tasks and responsibilities by commanders and staffs of different units are as diverse as the theaters of operation in which they are employed. Such diverse approaches are due to the absence of realistic doctrinal guidance required to establish standardization and unity of effort. In order for IO to be truly effective, commanders and staff at the operational level of war must ensure IO is considered from planning inception through execution-order development. This can be accomplished through an analysis of existing doctrine, doctrinal staff elements, their current capabilities and responsibilities, and their respective roles in mission planning and execution.

Joint Publication (JP) 3-33, JP 3-0, Army FM 3-0, *Operations* and FM 6-0, *Mission Command: Command and Control (C2) of Army Forces* provide the framework for aligning IO tasks with both potential and existing capabilities to determine areas of responsibility during the development of operational plans and the Military Decision Making Process (MDMP). The doctrinal guidance from joint publications is general in nature, focusing more on the creation and composition of IO cells and information management cells. Army publications,

although not perfect, provide a better understanding of the IO process and its relation to BC. After careful study of these publications, the overall assessment is that current doctrine concerning the planning and execution of IO is fundamentally flawed. The attempt to consolidate Army information tasks operationally while further distributing IO capabilities institutionally appears to be the product of a task-based approach to IO. In other words, Army doctrine looks at the nature of the IO tasks (e.g., attack, protect) and assigns them to where they seem to best fit into a staff, rather than looking at existing staff functional areas, technical expertise, and capabilities and assigning the Army IO tasks accordingly. The development of Army information tasks as core competencies in the staff sections/military occupational specialties where the capabilities already exist supports a more consolidated, yet still decentralized approach that better serves the adaptive planning process.

Army information tasks are found in FM 3-0³ and focus on producing different effects based on the capabilities employed. Information engagement uses not only special staff sections and special operations forces, but also soldiers and leaders on the ground, interacting with the local population both at home and abroad to influence the opinions and attitudes of those populations. Information engagement is also the process of sharing the Army's and the organization's story in accordance with the desired command message. The next two information

tasks reflect and apply directly to the increased focus on cyberspace and the risks and advantages of working within the virtual environment.⁴ Command and control warfare employs tactics to attack, through physical or electronic means, the C2 network of the enemy. The methods employed range from jamming cellular phone frequencies to air strikes on enemy communications assets. The inherent risks involved with operating in cyberspace, as mentioned above, require comprehensive and continuous information protection. Protecting our networks, communications equipment, and data is critical to achieving and sustaining information superiority. The fourth information task, OPSEC, is closely aligned with information protection. The constant counterintelligence and vigilant supervision of physical and electronic security of information pertaining to operations, plans, facilities and communications networks is crucial to denying enemy access to our techniques, tactics, and procedures (TTP) and SOPs. Finally, through the employment of military deception, commanders can quickly and effectively disrupt or usurp the enemy's planning and decision-making process.

The Army has made vast improvements in a short amount of time to existing doctrine, but the overall process remains somewhat confusing. Although information tasks are clearly defined and explain the "why" and "how," there is no clear explanation of "who" or "where." It is certainly implied that



Helicopter Delivered MISO (PSYOP) Leaflets in Iraq

Source: defenseimagery.mil

the responsibility for planning IO lies with the commander and staff, but doctrinally, there are no specific responsibilities assigned. This leads to the wide variety of approaches to the IO planning and execution process mentioned earlier (see Table 1). An examination of the staff duties and responsibilities in FM 6-0 reveals the reasons for the current state of confusion regarding IO roles and responsibilities.

It is important to note that in joint doctrine, staff organizations are built around a service component's existing staff, and there is no designated J-staff for IO as there is in Army doctrine.⁵ For example, the J-7 in a maritime component commander's typical staff organization is designated as the joint exercise division, while J-7 designates the engineering staff section in a joint force land component commander organization. Essentially, the capabilities, expertise, processes, and SOPs need to be integrated into the joint task force regardless of the Napoleonic letter-number designation. With that in mind, according to FM 6-0, the Assistant Chief of Staff (ACOS) G-7 section is responsible overall for IO.⁶ The G-7 also has coordinating staff responsibility for the military deception officer (MDO), electronic warfare officer (EWO), OPSEC officer, and military information support operations (MISO) officer (the first and third of which used to be additional duties of the G-6 and G-2 staff sections, respectively). Although well intentioned and possibly effective if put into practice at the operational level and above, the lack of an S-7 at the brigade

level and below can result in a confusing and disjointed effort at developing any type of IO plan based on operational-level guidance and directives effectively. Furthermore, the G-7 plays an extremely limited role in the overall scheme of IO. The G-7 scope of responsibility is limited to information engagement activities mainly through cooperation with civilian agencies, MISO units and the public affairs office (PAO). Additionally, FM 6-0 provides vague guidance on the G-7's targeting and planning responsibility, makes no mention of any elements from the four remaining IO tasks, and assigns coordinating staff responsibility for the PAO, a key player in information operations, to the ACOS, G-1.⁷

In practice, the actual capabilities for executing IO tasks are spread out and exist predominantly among coordinating and special staff sections and external organizations other than the G-7. For example, based on expertise and access to resources, OPSEC falls logically into the military intelligence realm of the G-2, while capabilities and technical expertise for electronic attack, computer network attack and other information-technology-related functions reside in the G-6 section. However, the G-6 is only responsible for information protection, information assurance, and network defense, which are limited in scope relative to all five Army information tasks. Such an irrational approach prevents effective injection of IO planning considerations during the MDMP and fails to suitably further the goals of BC. Without unity of effort, staff elements

Table 1-Typical Staff Alignment of IO Tasks and Capabilities

Army Information Task(s)	Staff Officer or Section(s)	IO Capabilities	Desired Effect
Military deception	ACOS, G-7 ACOS, G-5 ACOS, G-2	Psychological operations, counterintelligence	Exploit/Deceive Enemy
Information Engagement	PAO Mil Dec Officer PSYOPS Officer	Leader and Soldier Engagements; media engagements; distribution of mass media; Diplomacy (US and abroad)	Influence/shape public opinion; counter enemy propaganda
Command and Control (C2) Warfare	ACOS, G-3 ACOS, G-2 EWO	Counter IED; Electronic attack; network attack; computer network exploitation	Disable or destroy enemy information systems; disable enemy C2 assets
Information Protection	ACOS, G-6	Information assurance; Computer network defense	Protect information systems; ensure availability and protect data
Operations Security	ACOS, G-3 ACOS, G-2 OPSEC Officer	OPSEC; Physical security; JPAS; counterintelligence	Secure information; control access

are indirectly responsible and IO tasks become more implied in nature, rather than specified.

Clearly, any attempt to consolidate and integrate all of these capabilities into one single IO entity at the operational level is not only too complicated, it is also unnecessary. The solution requires a shift away from two paradigms common among Army leaders. The first is the notion that important concepts such as IO require a single subject matter expert, staff section, or functional area. This solution was applied to earlier organizational developments such as EW and knowledge management (KM). The result was the creation of two new Army functional areas and the assignment of dedicated knowledge management officers at the operational level and dedicated electronic warfare officers at both the operational and tactical levels. Army EWOs currently focus on installation, operation, and maintenance of vehicle-mounted systems that counter improvised explosive devices (IED). Knowledge management officers (KMO) generally manage software applications on servers along with the architecture and web-based design of each organization's data repository, commonly referred to as a portal. Knowledge management officers are assigned mainly at the division level and higher, and only assist and advise units at the brigade and battalion levels. The responsibility for KM at the brigade level and below predominantly falls on the S-3 section, while in other units the S-6 section is responsible. The second paradigm is the notion that anything to do with "operations" to include IO must be directly controlled and supervised by the ACOS G-3 and anything "institutional" directly by the chief of staff. For example, both EW and KM were originally the

responsibilities of the signal regiment and were assigned as additional duties to either a signal officer, a Department of the Army civilian, or a capable noncommissioned officer. Knowledge management officers now come under the direct supervision of the chief of staff which can preclude interaction with other coordinating staff members.⁸ And although *FM 6-0* assigns coordinating staff responsibility for the EWO to the ACOS G-7, IO section, in practice, both functional areas normally fall under the G-3/S-3, operations section instead. In situations where a functional-area qualified EWO is not available, the G-6/S-6 section is responsible for EW.

The most viable, logical, and easily implemented solution is to continue with a decentralized approach to Army information tasks, but realign them with the staff sections that are actually postured to implement the tasks into BC; that is, between the ACOS G-7, G-2, and G-6 sections (see Table 2). This will also require realigning the KMO and PAO staff sections under the ACOS G-7, the EWO under the ACOS G-6, increasing the scope of responsibility for EWOs and KMOs, and clearly defining roles and responsibilities during planning and execution. The new design consolidates duties and responsibilities under three coordinating staff officers in the rank of lieutenant colonel and also eliminates the need for further creation of functional areas, special staff positions, working groups, IO cells, functional coordination cells, and the like. Each staff section will incorporate the information tasks into existing staff estimates and annexes to the operations order and are responsible for updating the commander on ongoing IO during periodic update briefs.

This proposed structure assigns the Army information tasks of military deception and information engagement to the ACOS G-7, along with coordinating staff responsibility for the KMO and PAO. The ACOS G-7 would deal with any and all synchronization interaction with civilian agencies, non-governmental organizations, and external special operations forces such as MISO and civil affairs detachments. The addition of the KMO and PAO to the ACOS G-7 will establish unity of effort and improve control over the flow of information both internal and external to the organization. The KMO can provide the technical skills necessary for devising information flow and information sharing both within the unit and to the outside world, while the PAO provides the expertise necessary for functions such as constructing command messages, leader and Soldier engagements, and interaction with the media. This will better serve BC through the use of psychological effects in shaping the battlefield before, during and after operations and further facilitates the adaptive planning process.

Command and control warfare would become the responsibility of the ACOS G-6, in addition to the current responsibility for information protection. The knowledge and expertise of information assurance and computer network defense technicians can be readily applied offensively on the virtual battlefield. Hacking into and bringing down an al Qaeda website server or detecting a cyber terrorist during an intrusion detection alert and then tracing and attacking the invading system with a virus or worm program would enhance information superiority while deterring future threats or attempts to compromise our own systems. In

Table 2-Proposed Realignment of IO Tasks and Capabilities

Staff Section	Army Information Task(s)	IO Capabilities	Desired Effect
ACOS, G-7	Military deception Information Engagement	PSYOPS; PAO; KM; Leader and Soldier Engagements; Diplomacy (US and abroad)	Exploit/Deceive Enemy; Influence/shape public opinion; counter enemy propaganda
ACOS, G-6	C2 Warfare Information Protection	EW; Electronic attack; network attack; information assurance; computer network defense; Counter-IED	Disable or destroy enemy information systems; disable enemy C2 assets; protect own information systems;
ACOS, G-2	Operations Security	OPSEC; Physical security; counterintelligence; JPAS	Secure information; control access

addition to information systems and networking expertise, the G-6 is the proponent for radio frequency management and the procurement and use of both government and commercial off-the-shelf radios and other emitters. Furthermore, the G-6 has the personnel and systems in place to deconflict, report on, and control the entire electromagnetic spectrum from tactical and non-tactical ground communications equipment to space-based communications assets. Spectrum management is an area critical to electronic countermeasures and specifically key to the successful employment of counter-IED systems. To this end, the EWO would also be realigned with the ACOS G-6, consolidating under one section the offensive and defensive aspects of EW relative to both cyberspace and the electromagnetic spectrum found on the battlefield.

The fifth and final Army information task of OPSEC would remain under the capable and expert administration of the ACOS G-2. This makes more sense operationally for two reasons. As mentioned earlier, there is no S-7 at battalion- and brigade-level staffs; therefore, information dissemination, as well as pooling and sharing of resources between the G-2 and S-2, make OPSEC more effective, as opposed to the information being passed from the G-2 to the G-7 for dissemination to the brigade and battalion S-2. Likewise, the G-2 is better positioned to receive information and intelligence on real and potential threats as well as any existing and emerging techniques, tactics, and procedures being employed by the enemy.

Over the next 15 years, staffs at the tactical and operational levels should implement the IO structure described in this paper.



US Airman Setting Up Joint Command Post

Source: defenseimagery.mil

It should be standardized across the Army and added to future doctrine. This streamlined configuration effectively supports BC by better integrating information tasks into all operations. The design emphasizes staff section's strengths and aligns them with the desired capabilities to gain the desired effects from IO. Bringing IO assets under three distinct coordinating staff officers promotes unity of effort and clearer roles and responsibilities for each information task. The three-tiered approach conforms to institutional and operational requirements starting with the initial planning stages, throughout MDMP, and during execution. It requires minimal effort to put into action, requires no significant modification to existing task organization, and no new staffing requirements. Finally, the arrangement into three primary staff sections can be easily integrated into a joint task force construct quickly and eliminates the need for ad hoc working groups or cells. The proposed realignment and restructuring outlined above is just one possible way to adapt the current operational staff structure, capabilities, and core competencies to the demanding and complex landscape of IO. As the nation's enemies, nature of warfare, and information technology continues to adapt and advance, the processes for planning and executing IO must be continuously refined and tailored to anticipate and meet the operational challenges that lie ahead. ●

Endnotes:

1. Department of the Army, FM 3-0, Operations. (Washington, DC: Government Printing Office, February 2008), 7-2.2. <http://www.clausewitz.com/readings/Cquotations.htm>.
2. Ibid. 5-2.
3. Ibid. 7-3.4. 2010 Worldwide Information Operations Conference, Chantilly, VA.
4. John J. Kruzal, "Cybersecurity Seizes More Attention, Budget Dollars," *American Forces Press Service* (2010), <<http://www.defense.gov/news/newsarticle.aspx?id=57871>> (accessed on March 6, 2010).
5. Department of Defense, JP 3-33, Joint Task Force Headquarters. (Washington, DC: Government Printing Office, February 2007), III-10-III-13.8. <http://www.clausewitz.com/readings/Cquotations.htm>10.
6. Department of the Army, FM 6-0, Mission Command: Command and Control of Army Forces. (Washington, DC: Government Printing Office, August 2003), D-40.
7. Ibid. D-46.
8. Department of the Army, FM 6-01.1, Knowledge Management Section. (Washington, DC: Government Printing Office, August 2008), 2-3.



MAJ Jay Anson enlisted in August 1990.. He was commissioned into the Signal Corps through Officer Candidate School in May 2000. MAJ Anson has a Masters Degree in Management Information Systems from Phoenix University and a Bachelor of Science in Business Administration with a minor in Computer Studies from the University of Maryland. He is a graduate of the Signal Captain's Career Course, the Brigade/Battalion S6 Course, the Signal Officer Basic Course, Airborne School, and the former Jungle Warfare School in Panama. He is a veteran of Operation Enduring Freedom VII, Operation Iraqi Freedom II and 09-11, Operation Joint Guardian in Kosovo, and Operations Joint Endeavor and Joint Guard in Hungary, Bosnia-Herzegovina and Croatia

The Next Decade and Beyond: Foundational Force Development for a “New” IO

By

Mr. Jonathan Drummond

Editor’s Note: Force development and training of the IO force is a recognized area that needs improvement. There are several initiatives in DOD that are addressing this need. Mr. Drummond’s article provides a great primer for this conversation. This article was first published in a digital special issue of IO Sphere for the 2011 World Wide IO Conference.

FORCE DEVELOPMENT AND WHY IT MATTERS

INTRODUCTION: AN IO TALE OF EVOLUTION

Midway through the preceding decade, information operations (IO) was viewed primarily as the aggregate of five discretely identified core pillars. As the tide began to turn in Iraq, and as the Awakening movement took hold in 2007,¹ it became increasingly clear that IO was evolving and its operational components could not be so conveniently parsed. Documentation of IO offensives by Multi-National Division Baghdad (MND-B)² revealed success was the product of a number of interacting factors, including:

- intense, multimedia saturation of a limited audience or area—a “flashlight” approach,
- lucid effects-based, objective-focused command which featured IO as part of Combined Arms,
- vital (not merely supporting or related) roles for key/local leader engagement; public information and public affairs campaigns; on-the-ground face-to-face interactions; and pervasive message-consistent actions, and
- unity of effort.

Examples highlighting the evolution of IO from a few primary pillars to a complex process abound. In May 2008, Washington announced that the \$5 million bounty on Abu Ayuub al-Masri, leader of al-Qaida in Iraq, was being slashed to \$100,000. It appears that in reducing his value, the Coalition forces were able to send the message that Abu Ayuub was not competent.^{3,4} It seems to have worked, neutralizing Abu Ayuub, undermining his authority, splintering his followership, and increasing his vulnerability until Iraqi Security Forces (ISF) located and killed him in April 2010.⁵ Propagation of strategic communication via non-governmental conduits ultimately yielded a desired effect.

In another example, an enterprising team far from any operational role influenced the current leader of Al-Qa’ida! The Combating Terrorism Center at West Point published various informative documents in 2008-2009.^{6,7} The contents of these (and other) documents impacted at least some audiences and personally irritated Zawahiri; Zawahiri expended time and effort to counter CTC’s missives—importantly, this was time he did not devote to other destructive endeavors. An academic think tank had emerged as an influence asset.

The enemy has also become adept at conducting an IO chess match. On June 28, 2011, several attackers assaulted Kabul’s Intercontinental Hotel.⁸ Despite eventual defeat by Coalition forces, the Taliban successfully claimed victory. On the heels of President Obama’s announcement of an American drawdown, and days in advance of Kabul and other select areas being turned over to Afghan security forces, the Taliban sent a powerful message to Afghan audiences that Karzai’s government “can’t protect you.” Responsively, international media is carrying the U.S. and U.N. strategic communication that 80% of all civilian Afghan deaths are caused by insurgents.^{9,10,11} The “Taliban kills civilians” message may counter the Taliban effort to paint



Class Photo for a Senior Leader IO Course at Maxwell AFB Alabama

Source: defenseimagery.mil

coalition forces as murdering occupiers, but it will do little to counter the Taliban's messages about regime impotence and inability to protect Afghans in the wake of U.S. and coalition departure.

It is clear from the above that the "five pillars" approach to organizing and conducting IO must now yield to a more complex, multi-disciplinary, and integrated view. Those that conduct IO will need to master a greater array of tools, platforms, knowledge, skills, and abilities (KSAs) across all levels of operations. In a complex and rapidly changing information environment, we will be pressed to engage more aggressive and data-driven force development measures than ever before. IO force development will also need to produce professionals that are more innovative and creative. As Secretary of Defense Gates noted in January 2011, "Successful IO requires the identification of information-related capabilities [whatever they may be] most likely to achieve desired effects, and not simply the employment of a capability."¹²

A BRIEF PRIMER ON FD

The new definition of IO focuses not on discrete capabilities, but the ability to integrate a broad array of potentially effects-relevant information-related capabilities. It is also future oriented. IO is now:

"the integrated employment, during

*military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."*¹³

This suggests a needed expansion of KSAs throughout the IO force. Mastering application of a broad array of information-related domains implies the need to intensely train and educate a "new" Joint IO Force, and, in the process, professionalize it beyond the past paradigm in which a single course or experience often "qualified" a candidate. Recurring education and training toward competence and IO career development pathways are needed and will become the norm. The days of "one and done" course requirements are coming to a close and will not produce an expert, highly competent, and professionalized contribution to Combined Arms.

For the purposes of this article, force development (FD) is defined:

"The function of growing and managing a capable joint IO force. Growth is achieved by using a comprehensive education and training regimen that comprises interdependent supporting pillars of individual training, education, experience, and self-development;

*staff training; and collective training."*¹⁴

In the remainder of this article, the focus will fall heavily on training and education that supports achievement of the IO vision and capacity outlined by Secretary Gates in his 25 January 2011 Memorandum *Strategic Communication and Information Operations in the DoD*. Force management is also a major component of FD, but will be minimally addressed in the remainder of this article.

THE TIMES, THEY ARE-A-CHANGING

The new definition of IO lays down a contextual backdrop that obviates the need for a tight administrative clustering of a handful of capabilities. In fact, under the "five pillars" view, those focused on human behavior and perceptual realities (military information support operations [MISO], military deception [MILDEC], and operations security [OPSEC]) had always made for strange bedfellows with those focused more heavily on technological capacity (electronic warfare [EW] and computer network operations [CNO]). Information operations is undergoing a rapid change, and old proponencies are being split out. Joint Staff will now have integration and FD proponency across all IO, while USSOCOM, USSTRATCOM, and Joint Staff will parse the five capabilities previously forming the pillars of IO.



US Army MISO Soldiers on Patrol with US Marines in Afghanistan
Source: defenseimagery.mil

New challenges will arise, however, in this push to “normalize” IO, and to fully integrate a broad array of information-related capabilities (from a whole gamut of parent disciplines) into Combined Arms planning and execution.

First, the IO force will need to be familiar with a number of varied capabilities, their attendant limitations, and possible applications. An increasingly complex synchronization or integration function will require a new dimension to the training and education of planners—a specialization in piecing together coordinated, creative plans of attack, making optimal use of multi-tasked selections from an array of information capabilities assembled into volatile effects-achieving combinations.

Second, highly vertical and hierarchical command and control structures will fail. Information operations practitioners and planners will need expanded authorization to liaise directly, widely, and in real time.

Third, delegation in IO mission execution will be essential, and delegation of authorities will be highly desired to take advantage of real-time opportunities. One might imagine the coalescence of particular, almost modular, capabilities in a particular place for a certain period of time (the “flashlight” approach) after which the aggregate effort quickly dissolves, its components flowing into reconstituted IO efforts elsewhere in an area of responsibility (AOR). Simply put, the IO “zookeeper” now has a lot more animals in the zoo, and some will be herded together or partnered at various times and in ever-changing combinations or clusters. The training and education to prepare IO planners and integrators, to develop requisite levels of expertise and experience, will have to change to accommodate and optimize normalization.

THE IMPORTANCE OF “GETTING IT RIGHT”

We have thus far painted a vision of a new, more complex, and broader IO practice and mastery, along with initial insight into the education and training needed to ensure the command and integration of those faculties. We have seen that the field of IO is evolving rapidly, outpacing past definitions and conceptualizations. Still the reader may be asking just why such change to IO is necessary. There are two reasons.

First, in the coming decade, our national focus will be cast upon new and potential adversaries, novel situations, and other variations of nontraditional conflict. Shaping these situations and the information environment holds great potential to avoid the exorbitant costs of conflict we’ve seen in the last decade, and also to assuage the aftermath of conflict, natural disasters, and manmade humanitarian crises. Compared to some other instruments of national power, IO is a relatively inexpensive force multiplier that holds the potential to stave off the need for at least some expensive kinetic options and their consequences. We should do IO—and the FD supporting it—well in the interest of bolstering our economic position in the face of challenging growth and rising defense expenditures, especially in Asia,¹⁵ as well as preserve life and limit destruction and human hardship. In other words, we should do IO well if we hope to achieve mission success at minimal cost in a dynamic world.

Second, we should not do IO (and the supporting FD) poorly because there is a profound cost of not “getting it right.” Perhaps the greatest cost is engaging in conflict that might otherwise have been avoided. Another cost is losing domination of the information environment in such a way that national advantage or interests (e.g., economic, geo-political) are given over to potential opposition. A third cost is surrendering the arena



Afghans with Flyers

Source: defenseimagery.mil

of public discourse so as to allow the ascendance of fear, intimidation, and destabilizing nontraditional actors, be the Mexican drug gangs, the JANJAWED or Tehrik-e-Taliban Pakistan.

While the last decade has focused upon asymmetric threats, Rummel¹⁶ has clearly shown that the penchant for human destruction is far greater in the state exercise of violence. The Iranian theocracy, the North Korean dictatorship, and the Communist People's Republic of China remain high on the list of nations to watch as we face the coming decade. Democratic peace theory, the principle that democracies and democratic peoples do not wage war on each other^{17,18} suggests the importance of a long-term goal to ensure the triumph of democratic ideals and recent social phenomena like the "Arab Spring" or urban protest in the wake of disputed Iranian elections. The wide advance of democratic ideals and IO campaigns that further them is not just utopian well-wishing, but a long-term investment in less violent, destructive, and costly futures.

In the asymmetric challenges of the last

decade, lessons learned from Iraq and Afghanistan, the transition of U.S. global focus to emerging and evolving threats, and the on-going budgetary convulsions, there is an opportunity to "reset" IO, to define educational, training, and experiential pathways to professionalize the joint IO force for the challenges of a coming decade, and to explore cost-effective and sustained IO initiatives vested in desired strategic effects over the long run. Before turning more deeply to how we might "reset" the field, let's dig just a bit deeper into how the world is changing and the challenges an IO of 2020 must take on.

WHAT THE FUTURE MEANS TO IO AND FD

THE NEAR VIEW:

We have seen a steady decade of war, and while most of the focus has been in Iraq and Afghanistan, the battle of ideas and influence has been waged in hundreds of places around the world. We've come to realize that populations of interest appear to be arrayed across generally normal distributions. In the

tails of those distributions are people speaking out against violence, even at great cost, and on the opposite end of the spectrum, people who have chosen to indiscriminately destroy and kill. Between the extremes are the "fence sitters," and also those who are sympathetic to either extreme. LTC Vic Garcia had precisely this segment of the population in mind during an interview in Kandahar:

*"It's not just our side against their [Taliban] side, there's the population in the center - many of whom are sitting on the sidelines waiting to see who is going to come out on top."*¹⁹

It is the fence sitters and largely inactive sympathizers who are key to swinging area opinion and action in favor of democratic ideals or in opposition to violence, terrorism, and insurgency.

As the U.S. continues to draw down in Iraq, and as a reduction of forces begins in Afghanistan, the reduction of combat forces effectively lightens the kinetic hammer pounding at the violent tail of the above distribution. It is also the case that



Afghan Public Affairs and Media Officers Learn Use of Video Equipment

Source: defenseimagery.mil

the “budget is boss.” The belt-tightening in the Department of Defense has just begun, and it may be severe over the next 2-3 years. While domestic politics play out, undecided or inactive portions of the populations in Iraq, Afghanistan, and a litany of at-risk countries and regions will be subject to a barrage of competing influence attempts. IO, done professionally and patiently, constitutes a cost effective option that ought to remain available to decision-makers, joint planners, operators, and our allied counterparts.

FAR VIEW

As we look further into the future, peering out one to two decades, what does the future hold? What does it mean for IO? The National Intelligence Council’s 2020 Project and other reports provide insight.^{20,21,22} In the coming decades, major state-on-state conflict to the point of total war may be less likely than it has been at any time in the last century. Deaths from major conflict have been continuously declining since the 1950s. Peacekeeping operations have risen threefold, and use of sanctions with various levels of success is up 1400%. Clearly, in the nation-state arena, there has been a turn away from use of force; the welcome mat has been laid out for non-violent attempts to influence outcomes. This bodes well for the future and relevance of IO.

We might characterize the coming decades as ‘less death, more messes.’ Non-state actors, both conflict making and conflict resolving, will demand greater attention. The profusion of empowered actors will make things “messier” and multi-polar. Non-state organizations will accumulate greater leverage and power. Global firms will increasingly escape state control and be independent agents of change; indeed, since 2000, more than 50 of the top 100 economic entities globally have been corporations, not nations.²³ Information Operations will

therefore need to be directed at non-state and non-traditional targets.

Internationally, destabilization relevant to national interests will continue. Key resource-providing areas will become increasingly unstable, including Venezuela, West Africa, and portions of the Middle East. Transnational criminal power will increase, and its overlap with insurgency and terrorism will increase. Al-Qa’ida will likely be replaced by more adaptive Islamic extremists, patterned more tightly off arguably more successful models like the Muslim Brotherhood, HAMAS, and Hezbollah. Again, IO may be a cost-effective way in which to shape the environment and perhaps stave off conflict or disaster.

Kids, YouTube, Phones, and Guns

Modern technology is changing human interactions, and, accordingly, will influence what IO must be and do. Media, social networking, instant exposure venues like YouTube, and varied communications technologies will continue to shift power from states to individuals and non-state actors. People, not states, will increasingly be the agents of change. We will need to connect with them, sometimes over the objections of state leadership.

Some of these people will be younger than they were in past experience in conflict. Child soldiering has exploded in parts of Asia and Africa in the last 20 years. Underage youth have been enlisted into Al-Qa’ida’s North African and Somali affiliates and have been suicide bombers in Afghanistan. Further, there is a problematic “youth bulge” in a number of developing countries. The age threshold for influence target audiences can be expected to both drop and generate controversy.

As conflict moves into the cyber and other communications domains, IO will have to adapt both its activities and the



Afghan Man Takes Photo with Cell Phone

Source: defenseimagery.mil

platforms and technologies used. One person can now be far more powerful or influential than in the past. Rapid communications permit self-organizing adaptive social systems to sometimes outpace state authorities. For example, in the summer of 2001, “indigenous” Britons, south Asian Muslims, and police clashed violently over a period of many days in Oldham, United Kingdom. The ethno-religious conflict became quickly organized; using cell phones and runners, partisan neighborhoods were quickly and efficiently cordoned off and key intersections or urban terrain seized by the competing factions. It was a sign of things to come in places like Baghdad.

In a more benign example of virtual power, musician Dave Carroll sought restitution from United Airlines for damaging his guitar. He ultimately created a music video entitled “United Breaks Guitars,” and posted it on YouTube. Within 4 days, United’s stock tumbled 10%, costing shareholders an estimated \$180 million.²⁴ The joint IO of the future can’t ignore the potential of virtual power.

Think globally, act...INDIGENOUSLY:

Information Operations will need to appreciate the maxim to “think globally, and act indigenously”, not just locally. Amplifying credible indigenous voices and desirable messages will be part of this. Local innovation, rather than copied or transplanted solutions, has proven more successful in a broad swath of cultures. Business, civil society, and varied political

groups other than state powers will be future keys to stability-enhancing change. This has already been borne out in the evolutions of political culture in both Chile and Indonesia.²⁵

Population-centric vs threat-centric framing: It’s not a contest:

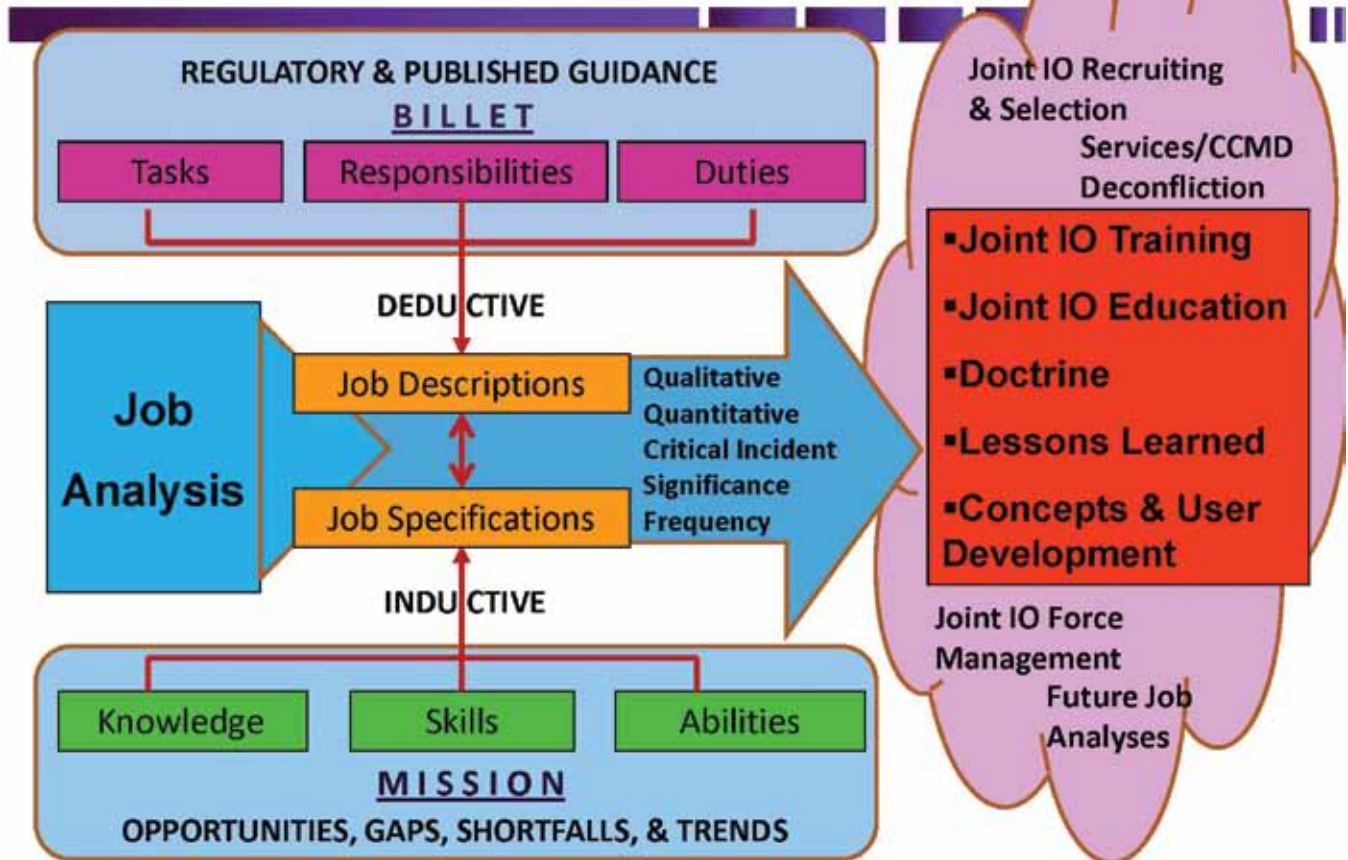
Admiral Olson and General Petraeus have advocated a population-centric framing of challenges to our national interests. As alluded to earlier, the population-centric approach recognizes the importance of “swinging” the undecided and inactive sympathizers in a population. Population-centric approaches may be expensive in some settings, but the cost of war, impasse, and alienation is arguably greater. To succeed, it may be wise to recall the promise of democratic peace theory, and consider IO that is focused on promoting principles that countries and people can appropriate as their own—e.g., rule of law, free choice of leaders, freedom of association and movement, accountability in governance—rather than imposing specific institutions or being too narrowly threat-centric.

We can’t just “drone” on:

Information Operations is a vital asset as a cost effective tool to further U.S. national policy. We cannot, during the withdrawal from Afghanistan, continue to just “drone” on. From the Wilton Park conference report cited earlier:

“...excessive force...serves to alienate the population. A

Comprehensive JA Approach



Comprehensive Job Analysis Approach
Source: Author

more minimalist approach to the use of force is required... Armed forces should also restructure and retrain for... modern conflict prevention and resolution. Capacity building and security force assistance will be required in greater numbers.”

All this points up a need for an IO encompassing a broad range of information-related capacities, complementary to the efforts of other U.S. agencies and NGOs, and empowering of traditional, more indirect special operations roles like security force assistance.

Possible futures: How must IO and FD change?

To summarize, IO will need to prepare for a future that is “less death, more mess,” a complex future in which agents of change and target audiences will proliferate; especially, the array of non-state actors and influence targets will expand. Force Development will have to keep pace with these changes. Joint IO professionals will need to connect with increasing numbers of youth and young people, and compete effectively and in real-time (i.e., fast, with delegated authorities, able to seize emergent opportunities) to move populations and areas of interest to desired perspectives and behaviors. The Joint IO portfolio will need to appreciate timely trends and find ways to execute influence operations via nontraditional social networking, virtual, and communications platforms. Intelligence support to IO will need to capture the nexus of both threat- and population-centric information, and IO integrators will need to apply that information to planning and execution that appreciates and is funded for long-term objectives. While IO will always need to support kinetic operations, IO stands to offer itself as a highly integrated, multi-dimensional, and

sometimes stand-alone capability that can evolve to realize its potential to achieve cost-effective effects and objectives, as compared to use of force.

INTRODUCING JOB ANALYSIS: A FOUNDATIONAL INVESTMENT IN IO FD DIRECTION FROM THE SECRETARY OF DEFENSE

The trend in IO away from discrete pillars and toward integrated aggregates of effects-achieving capabilities, the battlefield lessons of the last decade, and the array of possible futures suggest an urgent need to update the Joint IO Force—an imperative to train and educate practitioners, planners, and integrators to employ the lessons of the past and best practices while preparing for new challenges. In his January 2011 memo, Secretary Gates explicitly pointed out a current training-capability mismatch:

“... Combatant Commanders continue to stress the lack of adequately-trained IO personnel. It is imperative to recruit, train, educate... In this information-centric environment, IO training and education are particularly important.”²⁷

Considering the preceding outlay of active trends, growing complexity, and plausible futures, FD to reset Joint IO will, as a minimum, need to accomplish the following:

- Meet existing and forthcoming regulatory guidance;
- Educate across a non-redundant career progression: Service-bound apprentice or a Joint IO master;
- Address or correct IO shortfalls, failings, concerns, and challenges;
- Complement heretofore supported, supporting, related, and



Iraqi Officer Receives Certificate After Media Operations Training
Source: defenseimagery.mil

enabling capabilities as a contribution to Combined Arms;

- Make the most of battlefield successes, best practices, and lessons learned, and;
- Improve Joint IO Force expertise and recover tarnished credibility.

Key to the above is to structure Joint IO FD on empirically-derived data from the past and the best intelligence and trend analyses available. This is no small point. While well intended, the vast majority of IO schools in the DOD presently embrace curricula that have not been demonstrably linked to in-field tasks. Subjective impressions are no foundation for force preparation and professionalization.

JOB ANALYSIS TO SUPPORT JOINT IO FD

The only way to uncover the vast array of requisite tasks for any discipline and the KSAs necessary to do them is to conduct a comprehensive job analysis.²⁸ Only in this way can we determine the content and depth needed in Joint IO training and educational programming. One step in the job analysis will seek to determine the KSAs deductively from existing billets across the various commands and staffs. To be complete, the job analysis will also need to be future oriented to account for Secretary Gates' "potential adversaries" and future challenges. For this reason, an inductive inquiry that seeks to identify what tasks ought to be done per current and anticipated missions, battlefield lessons, future trends, and contingency plans must also be completed. Identified KSAs will cluster together into coherent tasks, and ultimately, will sketch out job specifications that will inform outdated, modified, or new job descriptions.

Both the deductive and inductive portions of the job analysis must appreciate certain aspects of the joint IO capacity to do particular tasks at varying frequencies. What are the critical incidents IO professionals face? What are the tasks that, while rarely done, are so important that there can be no tolerance for mistake or failure? Some easy, frequently performed, and relatively unimportant tasks can be trained on the job. Other difficult, infrequent, and important tasks may be perfect candidates for formal initial and recurring training.

The data gathered in this job analysis effort will impact FD in a number of ways. First, it will become the basis for developing education and training courses of action. The derived information will define the KSAs to be trained to and acquired by Joint IO professionals at varying levels. It will become the basis for Joint IO training standards and

qualifications. It may also be used to suggest education and training options which prepare the broader non-IO force and decision-makers for a Combined Arms integration of IO in planning and execution. Information derived during the job-analysis effort will inform the breadth and depth of KSAs associated with the gamut of "information-related capabilities." Finally, the data and follow-on efforts will be key to defining initial and recurring training to professionalize the Joint IO force across a career progression. In short, the days of "one and done" are over.

Second, the information from the job analysis could be used to better recruit or select Joint IO professionals. Some Services may better prepare their contributions to the Joint IO force than others; indeed, at present, only the US Army appears to have a methodical programmatic track for IO professionals.

Third, Joint standards and qualifications arising from a more defined career progression and the associated FD will ease some of the challenges of force management. It appears that sometimes combatant commanders did not realize they had received trained IO personnel, when in fact, IO personnel were not efficiently channeled into IO positions.

BUILDING-ON-THE-JOB ANALYSIS

Many aspects of solid FD stand on the shoulders of sound job analysis and inferences from that data.

First, FD will need to enable future joint IO professionals to "play well with others." Given the interdisciplinary nature of grasping a broad scope of information-related capabilities, it will need to be determined what level of familiarity or expertise is appropriate in any given domain. As one IO officer asked, "Will I need to take a strategic communication course? A public affairs course?" The answer to these questions is contingent upon just what tasks a joint IO professional is expected to do and what KSAs he or she needs to possess. A certain degree of expertise will be needed for an IO integrator to bring together the right mix of information-related capabilities to achieve desired effects at a certain place in real time.

Second, since IO now encompasses a range of information-related capabilities, we might well highlight the need to have "longer leashes for bigger dogs." To facilitate real-time decision-making, responses and exploitation of emergent

opportunities, risk acceptance will need to rise, risk aversion will need to decline, and authorities will need to be delegated to far lower levels than has been customary. Intense Joint IO FD and professionalization based upon a valid job analysis should go hand-in-hand with greater responsibility and more confident downward delegation of authority.

Finally, a solid job analysis should highlight those KSAs vital for executing the core challenge of most IO—reaching the target audience with an appropriate message or other stimulus to achieve the desired effects. In many cases this will involve meeting the target where they are; (sub)culturally, technologically, linguistically, and so on. A comprehensive job analysis should better capture some of the necessary talents to do this. Where indigenous values and U.S. interests are conflated, we should aggressively exploit the information and influence landscape, and train and educate IO professionals how to best do it. The approaches may vary widely by target audience and desired effect, but the move away from five IO pillars and a handful of gadgets to an approach which freely integrates effective elements of power is a move in the right direction.

LOOKING AHEAD

It is an unfortunate maxim of human nature that no one wants to fail in new ways, but they're more than ready to keep failing in "the same old ways." We can take comfort being ready to engage IO as we've done, or we can dare to dominate the information landscape by "resetting" IO, and the FD to support IO Force professionalization and expanded capacity, on the basis of a present-appreciating and future-anticipating job analysis which defines mission-essential KSAs.

As we've seen, IO is evolving for us, our friends, and our present and potential enemies. Information Operations can no longer be viewed as a stagnant capability set, but is better defined as a process that makes use of all applicable and appropriate resources and capabilities to contribute to and achieve desired Combined Arms effects. The trends of the future portend greater complexity, a profusion of potential target audiences, the ascendance of non-state actors, an expansion of media domains and platforms, and the potential for IO to be more acceptable as a cost-effective, long-term, less violent application of national elements of power.

Consider, for example, that the evolution of varied IO efforts on the part of the U.S. and coalition partners converges on certain interdisciplinary insights. In the MND-B “flashlight” approach mentioned earlier, target audiences or areas were essentially “blitzed.” Similarly, IO and other programs run by authorities in Algeria, the Kingdom of Saudi Arabia, and Singapore have successfully sought to take a multi-pronged attack to a resource-constrained terrorist or insurgent enemy.^{28,29,30,31,32,33}

At USSOCOM, LTC Garcia and I often discussed the need to punish the enemy by “flooding the zone” with our information, depriving them of the ability to respond, and exploiting precise instances of their inability to respond. As General Baker recently advocated in *Military Review*, high repetition and heavy dissemination of limited themes and messages in an operation marked by unity of effort is key to great IO operations. In all these examples, a few characteristics are common and subject to incorporation in FD:

- Flexible allocation of appropriate resources as the situation demands;
- Saturation and repetition;
- Unity of effort – little concern for planning by capability and greater interest in integrating whatever array of capabilities will best bring about desired effects and end states, and;
- Meeting, influencing, or overwhelming the opposition where they are geographically, virtually, and culturally.

The initiative to reset IO and the FD of the IO force begins with a comprehensive inductive and deductive job analysis. Done

well, it carries us past the battlefield failures, makes the most of battlefield successes, appreciates the past and lessons learned, promulgates identified best practices, accounts for evolving threats and developments, remedies shortfalls, anticipates future challenges, and stands to restore a tarnished credibility resulting in part from inadequate or incomplete training and preparation for (1) those who “do” IO, and (2) leadership trying to make optimal use of IO. Information Operations can become a ghost of the past, or it can realize its potential to be a cost-effective, integrated, flexibly structured, long-term instrument of national power.

Joint Staff J-7, Joint Staff J-39 and JIOWC J-57 (Under the Joint Staff J-39 1 October 2011) have recently launched the initial steps to undertake a comprehensive Joint IO Force job analysis funded by the Office of the Secretary of Defense. Future follow-on articles will update IO Sphere readers on the project and the details of its progress. ●

Endnotes:

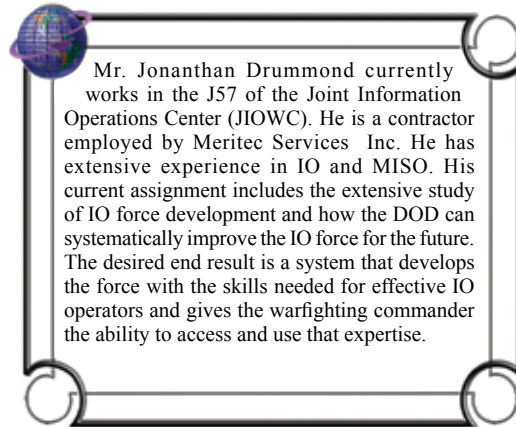
1. Cave, D., & Rubin, A.J. *Baghdad's weary start to exhale as security improves.* *The New York Times.* (November 20, 2007).
2. Zimmerman, F. H. *Attack, attack, attack: Information Operations: Multi-national Division Baghdad (4th Infantry Division), December 2007 to February 2009.* *IO Sphere, Winter 2010, 10-17.*
3. *U.S. News Staff. Why the US slashed bounty on a terrorist.* *US News & World Report.* (May 13, 2008). Available at: <http://www.usnews.com/news/iraq/articles/2008/05/13/why-the-us-slashed-bounty-on-a-terrorist>
4. *Mulrine, A., & Whitelaw, K. The U.S. quietly slashes the reward posted for the leader of Al Qaeda in Iraq.* *US News & World Report.* (May 12, 2008). Available at: <http://www.usnews.com/news/iraq/articles/2008/05/12/the-us-quietly-slashes-the-reward-posted-for-the-leader-of-al-qaeda-in-iraq>
5. *Bazin, K. R., & Meek, J. G. Top two Al Qaeda operatives in Iraq, Abu*



US Marines Conduct a Census in Afghanistan

Source: defenseimagery.mil

- Ayyub al-Masri and Abu Umar al-Baghdadi, killed: *U.S. New York Daily News*. (April 19, 2010). Available at: http://articles.nydailynews.com/2010-04-19/news/27062276_1_abu-ayyub-al-masri-al-qaeda-iraq-baghdadi
6. Helfstein, S., Abdullah, N., & Al-Obaidi, M. *Deadly vanguards: A study of Al-Qai'a's violence against Muslims*. (December 2009). Available at: http://www.ctc.usma.edu/wp-content/uploads/2010/10/deadly-vanguards_complete_1.pdf
7. Brachman, J., Fishman, B., & Felter, J. *The power of truth?: Questions for Ayman al-Zawahiri*. (April 21, 2008). Available at: http://www.ctc.usma.edu/wp-content/uploads/2010/06/Power_of_Truth_4-21-2008.pdf
8. Rubin, A. J., & Nordland, R. *Raid by Afghan forces and NATO ends attack on hotel in Kabul*. *New York Times*, p. 1. (June 29, 2011).
9. *Abi-Habib, M. Civilian deaths rise in first half in Afghanistan*. *Wall Street Journal*, p. 13. (July 14, 2011).
10. Michaels, J. *U.N. assails the Taliban over deaths of civilians*. *USA Today*, p. 1. (July 15, 2011).
11. King, L. *Afghan civilian deaths up 15% this year, U.N. report says*. *Los Angeles Times*, p. 3. (July 15, 2011).
12. Gates, R. *Strategic communication and information operations in the DoD*. (January 25, 2011).
13. *Ibid.*
14. CJCSM 3500.03B
15. *National Intelligence Council's 2020 Project. Mapping the Global Future*. Pittsburgh, PA: Government Printing Office. (December 2004).
16. Rummel, R. J. *Statistics of Democide: Genocide and Mass Murder Since 1900*. Charlottesville, Virginia: Center for National Security Law, School of Law, University of Virginia; and Transaction Publishers, Rutgers University (1997).
17. Hermann, M. G., & Kegley, Jr., C. W. *Balloons, a Barrier Against the Use of Bullets and Bombs: Democratization and Military Intervention*. *Journal of Conflict Resolution*, 40 (3): 436-460. (September 1996).
18. Rummel, R. J. *Power Kills: Democracy as a Method of Nonviolence*. Transaction Publishers, Rutgers University. (1997).
19. *Riechmann, D. Afghan, NATO forces brace for spring offensive against Taliban*. *The Washington Post*. (February 7, 2011). Available at: <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/07/AR2011020703651.html>
20. *National Intelligence Council's 2020 Project. Mapping the Global Future*. Pittsburgh, PA: Government Printing Office. (December 2004).
21. Brown, R., & Selvaduri, S. *Conference report: Global conflict-future trends and challenges: Towards 2030*. (April 2011). Available at: <http://www.wiltonpark.org.uk>
22. *Conflict trends issues. ACCORD: The African Centre for the Constructive Resolution of Disputes*. See <http://www.acCORD.org.za/publications/conflict-trends/downloads.html>
23. *Anderson, S., & Cavanagh, J. Top 200: The rise of global corporate power. Institute for Policy Studies*. (December 2000). Available at: http://www.ips-dc.org/reports/top_200_the_rise_of_corporate_global_power
24. *Ayres, C. Revenge is best served cold—On YouTube*. *The Sunday Times* (London). (July 22, 2009). Available at: http://www.timesonline.co.uk/tol/comment/columnists/chris_ayres/article6722407.ece
25. Brown, R., & Selvaduri, S. *Conference report: Global conflict-future trends and challenges: Towards 2030*. (April 2011). Available at: <http://www.wiltonpark.org.uk>
26. *Finel, B. Seven observations on the potential strategic implications of population-centric counter-insurgency doctrine*. *Small wars journal*. (August 2009). Available at: <http://smallwarsjournal.com/blog/7-observations-on-population-centric-coin>
27. *Gates, R. Strategic communication and information operations in the DoD*. (January 25, 2011).
28. *Knight, P., & Saal, F. Industrial/Organizational Psychology*. Thomson Brooks/Cole. (1998).
29. *Associated Press. Algeria steps up its war against Al-Qaeda*. *CBS News*. (March 2, 2009). Available at: <http://www.cbsnews.com/stories/2009/03/01/world/main4837117.shtml>
30. *Hunt, E. Counter-terrorism successes force Algerian militants to evolve. Jane's intelligence review*, 11-16. (June 2006).
31. *Hegghammer, T. There is nothing soft about Saudi counterterrorism*. *Foreign policy*. (March 11, 2010). Available at: http://mideast.foreignpolicy.com/posts/2010/03/11/there_is_nothing_soft_about_saudi_counterterrorism
32. *Boucek, C. Saudi Arabia's "soft" counterterrorism strategy: Prevention, rehabilitation, and aftercare*. *Carnegie Papers, Middle East program*, 97. (September 2008). Available at: http://www.carnegieendowment.org/files/cp97_boucek_saudi_final.pdf
33. *Personal communications, Dr A. al-Hadlaq, February and October 2009; Dr R. Gunaratna, February 2009*.



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>

Coming Soon to NIPRNet
AN IO COMMUNITY RESOURCE
ADVOCACY FOR IO



The Value of Graduate-Level Education to Information Operations

by

Captain Roy Petty, US Navy
Captain Stephanie Helm, US Navy (Retired)

Editor's Note: This article is one of the cornerstone articles for this issue. IO education and professional development of joint IO officers is extremely important to the IO force. CAPT Petty and CAPT Helm's views on the importance of the IO line of operation as part of the mainstream of joint officer education is an important contribution to the discussion of the future educational development of the IO force.

In the 1980's, the notion of a joint officer corps within the United States was met within the ranks with a good dose of skepticism at best – often with outright hostility. No “real” Soldier (Sailor) (Marine) (Airman) would believe this joint nonsense had anything to do with real warfighting. However, as a number of military missteps (such as the failed Iranian hostage rescue, the Beirut embassy bombing and the Grenada invasion) caused senior US leadership to wrestle with understanding root causes, a predominant area of concern focused on our lack of service integration. An impassioned

debate ensued among senior DOD officials and the highest levels of the government on this issue.¹ Many acknowledged that something needed to be done to improve the ability of the services to work together and to clarify the chain of command. Others viewed this as a danger to the effectiveness of the military services. When Goldwater-Nichols was finally enacted in 1986, many resolute officers paid little more than lip service to its intent, followed the law only as far as it required, sought waivers from Congress whenever feasible, and hoped their service would remain untouched by this political intrusion into military business.

With the evolving nature of warfare and the globalization of the battlespace considered against declining troop strengths, restricted budgets, and the demand for communication connectivity down to the tactical level, it is hard to find merit in the argument that Goldwater-Nichols was a mistake. Today “joint” is the standard mode of operations. In fact, many junior officers, especially if they served in Iraq or Afghanistan, wonder why they did not receive some rudimentary joint professional



Chairman of the Joint Chiefs of Staff General Martin E. Dempsey with Students at the Joint and Combined Warfighting School in Norfolk, Virginia

Source: defenseimagery.mil

JOINT ELECTRONIC WARFARE THEATER OPERATIONS COURSE



SAN ANTONIO, TEXAS

A joint certified information-related capability 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: jiowc.ew.training@us.af.mil.

military education (JPME) as part of their service-centric officer education at the O-1 to O-3 pay grades. While the services concentrate on essential service-unique, tactical competencies for much of the initial officer education and training pipeline, it is common to find joint concepts or capabilities included in many professional communities: joint planning processes, joint intelligence support, joint logistics, joint communications, to name a few.

Joint professional military education (JPME) should be credited as the motivating function that drove the integration of joint thinking into every component of effective joint operations. JPME builds upon the service and professional competencies of the military officer, or peer agency civilian, and links them to operational and strategic activities. JPME educates the student as a military practitioner as well as an

operational thinker², while enabling the officer or civilian to work more effectively or efficiently in broader endeavors. The Officer Professional Military Education Program (OPMEP), which governs JPME implementation at military higher education institutions, emphasizes the importance of leveraging all aspects of diplomatic, information, military and economic (DIME) elements of the government in order to achieve higher-level strategic objectives. JPME students learn how to engage the appropriate elements of national power, integrate these elements with an operational design in order to achieve supporting operational and theater-strategic objectives. After JPME, graduates return to their careers, better prepared to operate more professionally and effectively in either a service or joint assignment.

For most military officers, their JPME experience is their first formal exposure

to Information Operations (IO). While studying the importance of leveraging all the elements of the DIME in modern conflict, most students would agree that the “information” element of power has been a pervasive factor throughout the history of conflict. Before the term “information operations” was ever coined, the information environment was a key aspect of the battlespace. Yellow journalism in the Spanish American war, Nazi propaganda, and Allied deception surrounding D-Day, and command and control warfare during the Cold War are all examples of how information has been an integral aspect of the fight.

Students returning from tours in Iraq or Afghanistan today often express opinions of “IO” based on what worked (or did not work) during their stint. The usual suspects are roundly castigated: the media does not support the military and portrays every event in a negative

MAKE A DIFFERENCE JOIN THE FA 30 TEAM



Become a US Army IO Officer



The US Army Information Proponent Office wants active-duty officers from year groups 97-99 and 03-08 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, vincent.motley@conus.army.mil) or IPO Personnel Chief (913-684-9432, matthew.j.yandura.mil@mail.mil)**

CHECK OUT THE FA 30 WEBSITE

<https://www.hrc.army.mil/site/protect/branches/officer/MFE/InfoOps/index.htm>

or salacious light; State Department talking points directly conflicted with DOD talking points; the Public Affairs and IO turf battle caused so much indigestion on the staff that no one wanted anything to do with them; the adversary could lie or deceive without blinking an eye and no one held them accountable; Combat Camera images that could counter enemy claims took 72 hours to get released; leaflets were papering over local villages without any means to assess the effect on the population; cyber authorities are byzantine and delivery of effects take too long. Good-news stories are sometimes few and far between. Improving military operations in the information environment across the board is uniformly recognized as a critical requirement.

Just as senior leadership recognized the need to leverage graduate education as a means to drive “jointness” today, there is emerging consensus on the need to educate military planners and leaders on the concepts of information in warfare and as an integral element of the battlespace. The information environment is an indistinguishable aspect of the modern battlespace, a point that was clearly articulated by Gen Stanley McChrystal Commander, International Security Assistance Force, Afghanistan in the opening of his ISAF Commander’s Counterinsurgency Guidance with the statement that “the conflict (in Afghanistan) will be won by persuading (emphasis added) the population, not by destroying the enemy.” With this statement, General McChrystal clearly coupled the success of the ISAF mission with our ability to fight and win the information war. He went on to say, “we must think of offensive operations not simply as those that target militants, but ones that earn the trust and support of the people while denying influence and access to the insurgent.”

Across the spectrum of conflict, information is used to confuse or eliminate an adversary’s ability to effectively command and control subordinates, foster superior maneuver capabilities to outpace enemy forces, tell the narrative of a counterinsurgency operation to bolster local support, provide transparency and legitimacy to operations, and enhance situational awareness and command/control of forces. In addition, information is used to enable more effective analytic judgments of adversaries’ capabilities and intentions. The nature of warfare today is such that whether high-intensity combat or a highly motivated counterinsurgency, the commander is compelled to consider information in many respects. Information can be an operational factor on par with time, space and force, it can be an operational function unto itself, or it can be a component of traditional functions such as C2, fires, maneuver or intelligence. Military practitioners and operational thinkers alike must account for the effects of military operations in the information environment and must recognize that these concerns are not limited to military domains or military actors. The reality of contemporary military operations is that conflict is essentially won or lost in the information environment. It is not enough to simply “win the war” -- we must also win the peace. Thus, operations today are largely designed to influence an adversary to move beyond the prevailing point of conflict to agreement on a better state of peace. With this in mind, bridging the gap between our traditional mode of military operations and the effect of “kinetic” activity in the information environment is a necessity.

The problem is that, while many other areas relevant to operational level of warfare have a heritage in tactical or service-specific operations (such as intelligence, logistics, fires, etc.) where the commander can easily draw upon savvy tacticians,



US Marines Conduct a Staff Study and Walk of the Iwo Jima Battlefield as part of their Unit Professional Education Program
Source: defenseimagery.mil

information operations is seldom seen as a service-only action. The core, supporting or related capabilities exist at the tactical level, and in some cases, stand alone at the operational level of warfare. But the employment of joint military information operations using capabilities as an integrated and synchronized effort to support operational-level missions does not usually emerge until the Joint Component Command is established as part of the JTF or JFC operation. This is where the need for IO Graduate-Level Education comes into play.

Just as jointness was eventually inculcated into mainstream military thinking through graduate-level joint education, information operations must be mainstreamed into operational-level thinking as well. The OPMEP already provides some foundational guidance for the information environment, but this is only the first step in fostering a deep understanding of these issues in our future leaders. For this reason, graduate-level education in the area of information operations should be fully integrated in the JPME. Operational thinkers/military strategists, as well as IO professionals, require solid grounding to effectively meet the challenges required to fight and win in the global information environment.

For the future admirals and generals, their development as strategists and military professionals cannot omit issues of information in their foundational education. OPMEP objectives can be expanded to better focus curricula to examine information issues, not only as a larger part of DIME, but also as central to military operations. But these future leaders should have opportunities to delve more deeply into issues relating to the information environment as a part of their JPME experience.

Likewise, it is not enough for IO professionals learn the details of core/supporting/related capability planning and execution. By focusing on IO alone, the future IO leadership is at risk of failing to integrate with the operational design and fundamental elements of plan. The IO professional should have the opportunity to delve more deeply into issues of “information in warfare” as part of their JPME experience.

One important component to help understand and develop the theory and practice of “information in warfare” is a viable graduate-level education program for information operations. Commonly called IO GLE, the concept was called for in the 2003 DOD Information Operations Roadmap. In practice, it has matured somewhat inconsistently, depending on the focus of each DOD higher-education institution, the nature of the college and the seniority level of the students. It is not important that each program look alike; what is of paramount importance is that these programs provide the students a meaningful educational experience to develop their understanding of “information in warfare” in a way that complements the basic “required” curriculum. The uses of military information operations in contemporary operations, theory of communication and social networking, intelligence challenges, cyberspace technologies, and case studies, which focus on the military use of information, are all good candidate topics for coursework. There are more issues than available class hours. The goal of IO GLE is to provide the opportunity to dig into issues affecting military operations and the information environment. The critical factor of IO GLE is the requirement for the student to think and write deeply on these issues, contemplating warfare in a way that encompasses the whole of the conflict beyond bombs and bullets. Whether the student is a military generalist or an IO professional, the process of researching and the formulation of perspective in this area of warfare is the true value of the IO GLE program. A beneficial by-product is the increase of

academic writings adding to the body of knowledge that further stimulates theory and doctrinal development.

DOD is constantly evaluating and updating the guidelines in the OPMEP as best practices from current conflicts are assessed. The OPMEP should continue to set standards for issues relating to the information environment as appropriate. However, beyond this “baseline”, DOD should make a firm commitment to develop viable graduate-level programs that provide an emphasis on information operations. It is imperative that IO GLE is supported as a high priority across all DOD higher-education institutions in order to better prepare future leaders, regardless of professional community, to meet the evolving challenges presented in the information environment. 🌐

Endnotes:

1. *Victory On The Potomac: The Goldwater-Nichols Act Unifies the Pentagon*, James R. Locher and Sam Nunn.
2. Vego, Milan, “There’s No Place Like Newport”, *Proceedings*, Feb 2010, p. 39.





**JOINT INFORMATION OPERATIONS
WARFARE CENTER
INFORMATION OPERATIONS
PRIMER COURSE
FOCUS**

- IO CORE CAPABILITIES AND PLANNING SUPPORT
- IO EXECUTION SUPPORT AND SYNCHRONIZATION
- JOINT PLANNING AND IO KNOWLEDGE BASELINE
- IO DOCTRINE AND OVERVIEW OF IO TOOLS

INFORMATION

- OPEN TO IO PROFESSIONALS BASED ON PRIORITY
- COURSE IS 4 DAYS IN DURATION

CONTACT: Mr. Michael Broster at 210-977-4701(DSN-969)
michael.broster.1@us.af.mil



Trouble on the Airwaves: Countering Radio Propaganda in Information Operations

by

Major Lynn Berg, US Air Force (Retired)

Editor's Note: This article deals with the importance of electromagnetic spectrum management in Military Information Support Operations (MISO) and how MISO must coordinate with Electronic Warfare to be as effective as possible. The article also deals with the need to continue to understand terrestrial radio operations in MISO and be able to utilize this technology even in the digital age. Major Berg's contribution is an important addition to the dialog on these issues.

The march toward a global information society appears to be well under way, with the promise of universal broadband access, merged cellular and wireless networks, and progressively more capable data standards. Proponents of these technological advancements often declare how digital systems will soon supplant traditional forms of mass communications for news and information. Yet a range of factors hinders a universally standardized telecommunications regime, still allowing traditional formats to endure. Analog radio, for instance, faces robust market challenges, but still persists in many parts of the world as the primary means of receiving information. Radio's rich tradition as provider

of information and entertainment has come with a parallel legacy as a source of disinformation and propaganda, which is currently reasserting itself in some regions of US security interests. Information Operations (IO) planners, typically absorbed in crafting deliberate strategies and products, must not lose sight of the need to monitor, gauge, and respond to radio broadcasts (both internal and external) that negatively affect the information environment. Systematic collaboration between intelligence and IO specialists will be required to identify the most harmful radio broadcasts and give commanders options to neutralize them.

Pitfalls of the Digital Wireless Age

It would be a fallacy to extrapolate our experiences as consumers and members of a tech-savvy society as a universal phenomenon. The barrage of advertisements for 3G, 4G, broadband wireless, iPhones, iPads, etc, might make it hard to fathom how a quaint technology like radio could survive as a significant means of information dissemination. Despite the massive popularity of global wireless communications,



US Marine IO Officer and US Army MISO Soldier Carry a "Radio In A Box (RIAB)" Transmitter for MISO Operations

Source: defenseimagery.mil

geographic, economic, and political factors still limit the predominance of digital wireless networks in many places. These limitations create wireless gaps where radio's intrinsic advantages are elevated. A brief characterization of these limiting conditions should help put wireless media in perspective, enhance analysis of specific information environments, and aid in the prioritization of media analysis.

The fundamental signal properties of wireless standards (802.11/802.16) and cellular systems make them essentially short-range communications. Virtually all wireless signals have free-space propagation range limits from meters to tens of kilometers due to higher frequencies, low transmitter power, and signal reflectivity. Seamless wireless access requires an extensive antenna network. The advent of satellite-based Internet hosting, such as Very Small Aperture Terminal (VSAT), promises to greatly spread and gap-fill wireless access in remote areas; however, associated costs also remain a consideration.¹ Meanwhile, radio's signal properties—lower frequencies and higher wattage outputs—generally ensure reception across much broader areas; e.g., global, in the case of shortwave. Terrain also constitutes a significant physical factor in determining both wireless and radio line-of-sight reception.

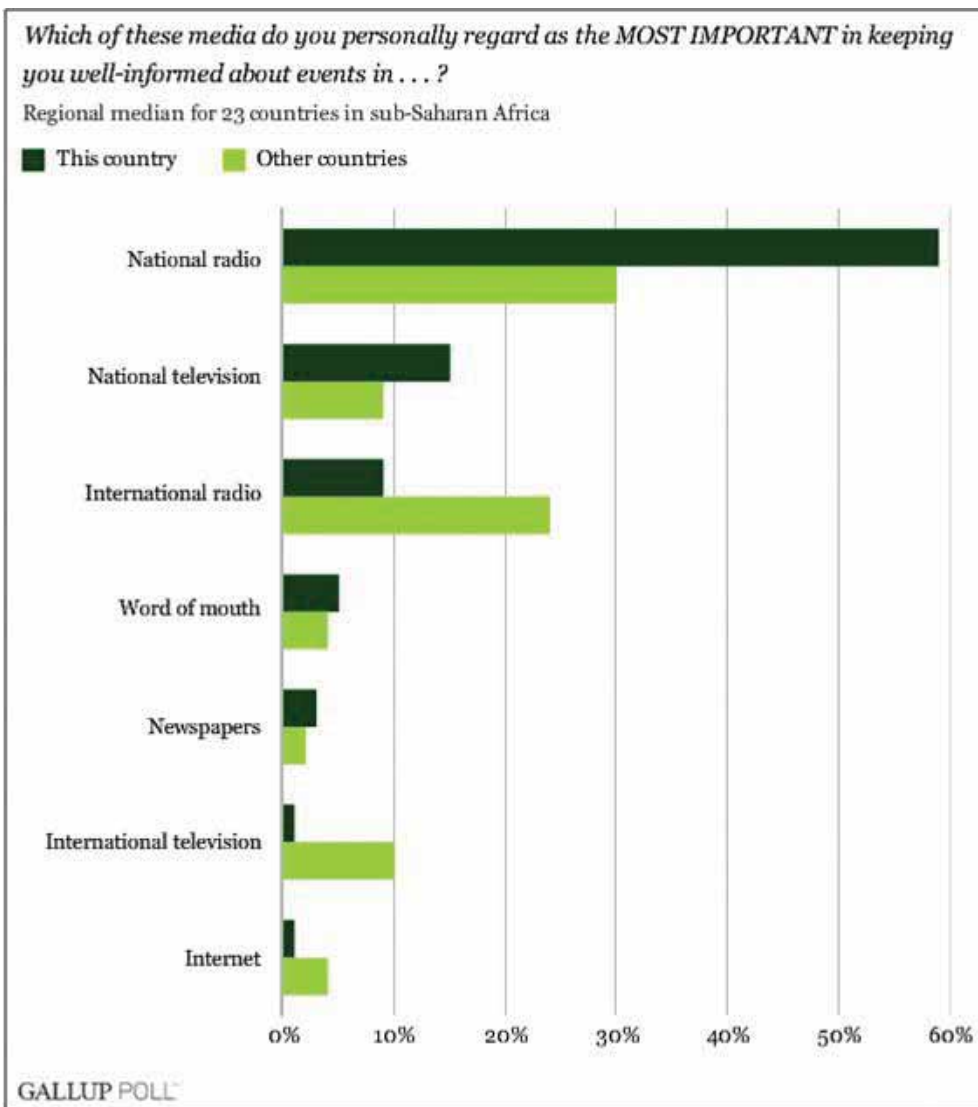
Economics also influence government and industry decisions to extend the wireless infrastructure. Companies face an important business decision in projecting where network expansion will be commercially viable. Wireless and cellular equipment components are costly to acquire and maintain, requiring vendors to conduct cost/benefits analysis before expanding service. Wireless access usually requires subscription or service fees, and the current devices, such as computers, phones, and personal digital assistants (PDA), are prohibitively expensive to many poorer families. Even in areas advertising "Free Wireless," somebody has to absorb the costs. For the consumer, terrestrial radio continues to be one of the cheapest forms of communication around the globe, requiring only

the one-time expense of a radio receiver.

Finally, wireless networks may exponentially increase the information "openness" of a society, a feature that can distress autocrats. Since companies need government approval to construct and expand each network node, suppressing the physical architecture serves as a highly effective means of controlling information. Saddam Hussein tightly controlled internet access and forbade cellular telephone networks, fearing their potential for subversive coordination of opposition forces. Radio transmissions, conversely, can be exceedingly difficult to block or restrict, since they rely so little on physical apparatus. This phenomenon has already played out many times in history, where external radio broadcasts have been able to penetrate the foggy interiors of repressive regimes. At the sub-national level, zealous religious groups may

denounce secular, commercial wireless services, and steer their followers toward more acceptable religiously themed radio broadcasts.

These constraints on wireless propagation mean that radio may still provide a cheap and reliable means of information particularly in isolated and underdeveloped areas. This is illustrated by a recent Gallup poll of Sub-Saharan African nations, asking people which media was most important for keeping them informed of important news events (see figure below).² In Somalia, the power of radio has led to a propaganda battle waged over the airwaves between government forces and the radical al-Shabab militia group. Both the government and al-Shabab are tapping into a culture in which entire families across the sprawling, arid country huddle around radios for news



Gallup Poll of Sub-Saharan African Nations

and entertainment.³ Not all regions depend upon or value radio as highly; indeed, the contemporary significance of radio as an information source varies depending on a multitude of factors. However, IO planners should not underestimate radio while initially gauging media preferences in conflict areas. Unfortunately, it is very possible that indigenous hostile forces would fully recognize the local preferences and get into those media/information sources early as part of their own information operations.

It should also be noted that catastrophic events, such as natural disasters and armed conflict, could cripple vulnerable wireless infrastructure, altering the normal communication patterns. In Haiti, the immediate means of communications support for earthquake rescue efforts fell on Amateur, or “Ham”, radio operators after the collapse of wireless networks. Combat operations can also greatly impact the connectivity and capacity of wireless networks. When the civil telecommunications architecture becomes part of adversary command, control and communications, it may be progressively degraded through our own targeting efforts. Insurgent forces may also choose to target communications infrastructure. Some Taliban leaders have decreed GSM tower shutdowns within their region of influence. They accuse the cellular providers of colluding with ISAF forces and vigorously target cell masts and offices, as well as kill maintenance workers.⁴ The result has been fragmented and unpredictable cellular service throughout much of Afghanistan. IO planners should anticipate the probability of wholesale or partial retrograde to radio dependence when existing wireless service is degraded.

Licensed Radio Broadcast

In early radio history, various organizations formed to create spectrum protocols to guide radio manufacturers. Since 1927, the International Telecommunications Union (ITU) has regulated the international radio spectrum, designating spectrum bands for “Services.” The frequency bands allocated for primary “Broadcast” services to the general public include the following:

Long-Wave band (amplitude modulation [AM]; 148.5 KHz – 283.5 KHz): Long wave is used for radio broadcasting in Europe, Africa and parts of Asia, and is not allocated in the Western Hemisphere.

Medium-Wave band (AM; 520 KHz – 1610 KHz): The ITU also authorizes the extended AM broadcast band between 1610 kHz and 1710 kHz in the Americas. This is the “AM radio” that most Americans understand.

Short-Wave band (AM; 1.711 MHz – 30.0 MHz): Short Wave allocation is divided into 15 broadcast sub-bands, with separate services designated for the interval bands. Short wave utilizes sky-wave propagation exploiting an atmospheric property called “ionosphere skip”, and is used by audio services intended to be heard at great distances.

Frequency-Modulation (FM) Broadcast band (88-108 MHz): Frequency modulation allows for stereo broadcast and clearer signal, but ranges tend to be shorter than lower-frequency AM bands.

The Federal Communications Commission provides a host of regulatory and oversight functions for the U.S. government, including regulating broadcast licenses, transmitter power levels, wireless media, digital transformations, and many other aspects of domestic spectrum use. There are

similar regional and national spectrum/communications regulatory groups around the globe; however, many are frustrated in achieving the desired level of oversight. Pakistan, for instance, regulates communications through the Pakistan Telecommunication Authority, but struggles to comprehensively control national spectrum use. They were recently compelled to install spectrum-monitoring stations in order to get a handle on unlicensed and interfering emissions from the Federally Administered Tribal Areas, Baluchistan, and the North-West Frontier Province.

Unlicensed Radio Broadcasts

The spectrum “Wild West” of many underdeveloped nations provides fertile ground for broadcasting outside established rules. That is not to imply that all unlicensed broadcast will consist of propaganda; music, news, and entertainment may also be delivered unfettered by license obligations. However, operating outside radio conventions greatly expands the potential for propaganda broadcasts, limited only by money, equipment, and radio receivers. A creative adversary, unmindful of legal or spectrum management obligations, may employ any means of broadcast.

This situation has fully presented itself in the Afghanistan-Pakistan (AFPAK) region, where Taliban and anti-government groups have embraced low-power, unlicensed FM radio broadcasts. “In the tribal areas of Pakistan, for example, there are only four legal FM radio stations, compared with more than 150 illegal low-watt stations run by militants, according to officials involved in the counterpropaganda effort. Some insurgent radio stations are mobile, broadcasting from vehicles or even donkey carts to avoid detection and extend their reach.”⁵

These broadcasts fill a void in areas lacking wired and wireless access. “There aren’t many sources of entertainment and information in this region. FM radio is an easy - and in some cases the only - option people have,” says Khadim Hussain, a research fellow at the Peshawar-based Ariana Institute for Regional Research and Advocacy.⁶ Setting up an illegal FM radio can be cheap and easy. All you need is a transmitter the size of a small box and an antenna that can be put on a tree or a minaret. The cost of these FM transmitters ranges from \$60



Amature Somali Broadcast Station

Source: Author

to \$185. Mountainous terrain may help channel these unlicensed low-power FM broadcasts into targeted valley settlements and evade detection by government agencies.

It would be a reasonable assumption that broadcast radio intended to reach an audience rather than an individual would occur only in frequency bands allocated for “Broadcast” services. However, radio bands intended for alternate purposes could be likewise utilized, depending on distribution of receivers. For instance, international spectrum allocations for Fixed, Mobile, Land Mobile, Aeronautical Mobile, and Maritime Mobile services are intended for point-to-point communications. These types of radios are sold by a multitude of commercial companies (e.g., ICOM, Motorola, Kenwood, Relm) and can be fixed, hand-held, or installed in vehicles/vessels. Synchronizing more than two receivers to a common frequency essentially creates a minor broadcast network. Several spectrum

bands are also allocated for Ham radio use. Ham radio has worldwide reach, and is a service for duly authorized individuals interested in radio technique solely with a personal aim and without pecuniary interest. While Amateur transmitters can be expensive, basic Ham radio receivers are relatively inexpensive and easy to operate. With coordinated times and frequencies, amateur radio can also serve as a home network for news, music, and entertainment.⁷ Ad-hoc radio networks established in non-broadcast frequency bands could be extremely flexible and likely difficult to detect among the clutter of other authorized users.

Countering Radio Propaganda

The challenge for IO teams is to recognize and respond to damaging radio broadcasts in a timely manner. Waiting too long to monitor and gauge effects on respective populations relinquishes information and spectrum control to the adversary. In Afghanistan, the pressing attention

on kinetic operations and improvised explosive devices has resulted in a laggard understanding of the political, cultural, and information environments. “Concurrent with the insurgency is an information war,” said Richard C. Holbrooke, the special representative for Afghanistan and Pakistan. “We are losing that war...The Taliban have unrestricted, unchallenged access to the radio, which is the main means of communication,” he added. “We can’t succeed, however you define success, if we cede the airways to people who present themselves as false messengers of a prophet, which is what they do. And we need to combat it.”⁸

Countering radio propaganda should be viewed as a targeting process, utilizing the battle-proven cycle of “decide, detect, deliver, and assess.” Initial planning should center on formulating guidance to shorten decision cycles and nominate radio broadcasts as targets. Information Operations planners should become familiar with international and national broadcast regulations,



Radio Station in Afghanistan

Source: defenseimagery.mil

existing broadcast stations and their charters, the commander's information objectives (along with supported/host-nation information objectives), coalition capabilities (and how to deploy to theater if not already in place), and even potential avenues for funding radio stations. Radio station directories can be found publically and on the Internet, and the Joint Spectrum Center maintains an extensive list of country studies, which depict national spectrum use, telecommunications, broadcast stations, and defense spectrum structures. A survey of the radio landscape in advance of operations can help cue intelligence and IO specialists on a monitoring strategy. For example, if an opposition group establishes, funds or takes control of a radio station, their programming will likely merit attention and probable response during operations.

The decision process to target a specific station may be aided by guidelines on when broadcast content tripwires from persuasion to threat. "Propaganda" is one of those seemingly self-explanatory terms that become less clear when scrutinized. One dictionary defines propaganda as

"The systematic propagation of a doctrine or cause or of information reflecting the views and interests of those advocating such a doctrine or cause."⁹ In a narrower and more common use of the term, propaganda refers to deliberately false or misleading information that supports a political cause or the interests of those in power. Propaganda is a form of manipulation, which exploits people, thinking, or capabilities. It does this by affecting the prism through which an individual's values, stereotypes, or interests are processed.¹⁰ Manipulation is a common objective of many domestic and international radio broadcasts. Offensive and misleading radio broadcasts may in fact be licensed, sanctioned by an authority, and contain elements of truth. Even most licensed shortwave services (3-30 MHz) are designed to serve political or religious interests.

When manipulation becomes a threat to mission or personnel, it transitions to harmful propaganda. Some radio content is overtly threatening to US missions; e.g., directions to harm or attack, instructions on making or using weapons, exhortations of violent action,

coded command signals. The parlance of many extremists, however, couches threatening language within euphemisms, analogies, religious scripture, and political criticism, greatly challenging the analyst. For instance, do zealous religious broadcasts constitute a threat? Do broadcasts that contain ethnic slurs threaten the mission? Are biased media broadcasts such as those, exhibited daily during Kosovo operations worthy of a commander's attention? When does inflammatory rhetoric become a threat to operations? Determining the effect of insidious propaganda is the keystone to pursuing an operational response. The commander should determine whether response will be triggered by certain key, demonstrable effects, or whether any and all offensive transmissions must be squelched as a threat to freedom of operations.

Radio broadcasts during the Rwandan genocide illustrate both the chilling depths of ethnic hate-speech and the ambiguities in determining radio's culpability for mass-murder. In 1993 Hutu backers established FM radio station RTLMC (Radio-Television



US IO Officer and Afghan Broadcast Director Conduct Coordination Prior to a Broadcast
Source: defenseimagery.mil

Libre des Mille-Collines-also known as “Radio Machete”) which stayed on the air for over a year. The RTLMC routinely broadcast anti-Tutsi hate-speech, using the term *inyenzi* (cockroach) to dehumanize the Tutsis, and going so far as listing by name who “deserved to die” and urging listeners to call in and reveal where Tutsis were hiding. The U.S. debated responding but stumbled over limiting free speech, differing interpretations of employed euphemisms, and the fact of discreet Rwandan government financial backing. Ultimately, the US ambassador in Kigali concluded that the legal radio station had a right to broadcast, and no attempts were made to shut it down.

Detecting broadcasts of interest requires a fusion of various intelligence disciplines, primarily signals intelligence and human intelligence, but possibly much open-source intelligence, as well. The effect of corrosive radio broadcast in all potential bands will need to be reported, analyzed, and assessed for targeting potential. This requires not just reporting “red” activity, but determining its overall effective on “white”; i.e., target populations. Intelligence professionals should cull information from their regions and up-channel it for corroboration at Joint Intelligence Operations Centers, which can to piece together disparate intelligence reports towards a more coherent understanding on radio influence. Monitoring unencrypted radio transmissions requires no sophisticated technology; however, prioritizing resources may require active

IO cell direction. Human Terrain Teams, when employed, may also be able to help gauge the local impacts of radio transmissions.

There are two primary dimensions to countering radio propaganda in an operational area: counteracting the content (message), and countering the transmission (means), both of which must be weighed against the commander’s desired information end state. A “counter-message” strategy may overlap and complement the Strategic Communication strategy, realizing that US strategic goals towards opposing certain political broadcasts may differ from the operational criteria to target such broadcasts. Establishing US-controlled, or nationally operated, but US-supported, high-powered AM, FM, or shortwave stations can create an outlet for enduring counter-message media strategy. The ability to broadcast across wide swaths of territory via national radio can provide counterpoint to other AM or shortwave offerings, and directly challenge numerous lower-powered nuisance FM stations. Particularly in remote areas with limited communications, these types of radio operations may be important in asserting government legitimacy and dispelling rampant disinformation that inherently harms the operational mission. In situations where the US objectives are primarily to enable and empower foreign governments, it may be crucial to mask US involvement. However, establishing permanent radio stations can require significant resources



Broadcast Professionals in Afghanistan Hold Meeting on Broadcasting Techniques

Source: defenseimagery.mil

and commitment, including equipment with trained operators, native language speakers, communications staff, and recurring operations and maintenance funding. In some scenarios, international organizations may also be leveraged. The U.N. has realized over decades of peacekeeping operations the degrading effect of propaganda broadcasts, and has recently invested resources in Somalia to offset al-Shabab-controlled Radio Warsan broadcasts. “As the propaganda war intensifies in the battered Horn of Africa nation, the government is using a newly modernized radio station to get its own message across to more Somalis, and the U.N. is financing a new radio station. When Somalis tune in to the government station in insurgent-controlled territory, they tend to do so in secret to avoid being punished by the al-Shabab rebels, who routinely execute suspected government collaborators.”¹¹

Military information support operations (MISO) teams will likely become the hub for tactically focused (i.e., temporary) counter-message operations, synchronized with other MISO products (e.g., TV, leaflets, posters, print media). Traditionally, most radio MISO broadcast has been handled by an airborne platform, the EC-130J (previously EC-130E) Commando Solo, a capable asset with a wide array of transmitters to handle multi-band broadcast. The Commando Solo is a low-density, high-demand asset; however, with extensive operating costs (i.e., fuel and flight hours), that may not be available for all situations. More recently, the ability to inject approved MISO messages on low-power FM systems has been greatly aided by the development of Radio Systems in a Box (RIAB). These portable systems contain all the equipment necessary to have a stereo FM, and sometimes AM, radio station up and running within minutes. Different systems contain different inputs, but connecting to a laptop computer provides great flexibility in programming, and possible round-the-clock broadcasts. Automated programming allows for persistent broadcast of music, news, key leader speeches, medical alerts, poetry, and even daily prayers in areas where such output is important. Live DJs, when available, create an exciting opportunity to engage target populations with call-in shows, current news items, and responsive programming. Increasingly, feedback from RIAB listeners has demonstrated the payoff of culturally tuned content. Ignoring local ethnic and cultural desires runs the risk of souring target populations into dismissing such offerings, resulting in wasted time

and effort. When properly done, these tactically employed radio stations can provide an appealing alternative to tiresome government or opposition fronted radio broadcasts.

There have already been many successes using RIAB throughout Afghanistan by Army and Marine units. One example includes dual radio stations set up by the Georgia Army National Guardsmen of 1st Squadron, 108th Cavalry Regiment, in the Shinwari and Muhmandari Mountain border village. Both stations are fully funded by the coalition with Afghan National Security Force partners offering

security, and employ full-time local Afghan station managers and on-air personalities. The “Afghan face” of these stations greatly increases their likelihood of effectiveness, and provides local officials with another means to assert their own information objectives. “It will not be a facilitator of military or security mandates,” Afghan Border Police, 6th Kandak commander, Col. Niazy said. He punctuated the importance of the mission by stressing how the station’s messaging will embrace the needs of the community. “It will be a powerful tool to give our people a voice - a resource. Our mullahs, district government leaders, or our local



Afghan Border Radio Station at Police Facility
Source: author

shopkeepers and villagers will have full access and know that they can come to us in a crisis for honest information.”¹²

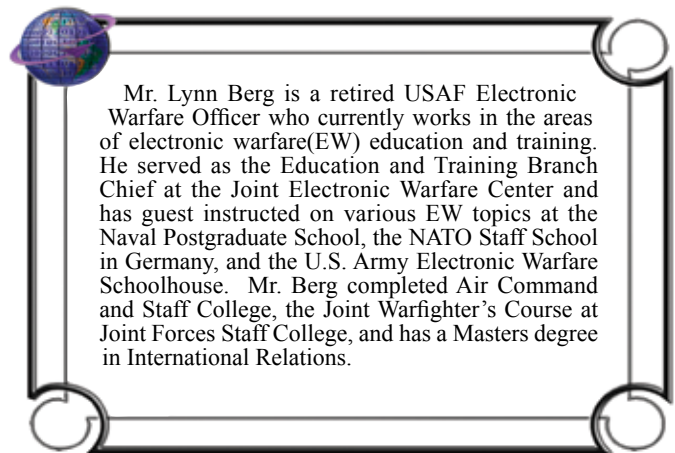
Countering the transmission means through jamming is another option, but available jamming equipment may not provide the necessary persistence or appropriate waveforms, as the majority of jamming equipment was not designed for countering radio broadcast. Jamming may also run the risk of interfering with or overlapping legal and government FM frequencies. A more productive option might be to establish a countering radio broadcast on of the same frequency as the offending broadcast, essentially jamming the signal, while also disseminating approved messages and news. When networks are established across tactical radio bands, the only viable option may be to jam the signal using standard tactical communications jamming equipment. Radio-frequency (RF) propagation modeling can greatly assist in the planning and employment of transmitters, particularly if combined with cultural and language overlays. The more vertical the terrain, the more RF propagation modeling can help ensure transmission effectiveness.

Radio propaganda has been utilized in nearly all modern wars as an attempt to manipulate troops and lower morale. “Axis Sally,” “Tokyo Rose,” and “Hanoi Hannah” attempted to sap the fighting spirit of the U.S. military across an entire theater of operations, leaving lasting impressions but with debatable results. Even as radio’s primacy as an information source has waned in technologically advanced regions, political and military groups have continued to leverage the medium’s advantages in remote and underdeveloped regions. A subtle shift may be occurring in employment strategy, as well. In many instances, radio has become more militant, employed as a means to directly sway, influence, or intimidate crucial segments of the population within the boundaries of existing coalition operations. Adversary use of radio as a means to coerce supporting key leaders and populace, as well as directly threaten coalition operations, demands decisive IO to maintain our operational advantage. ●

Endnotes:

1. *Other strategies and technological approaches are being explored to ensure wireless access in remote areas. Universal Access & Service Agreements, lower cost equipment, and innovative use of repeaters and low cost routers provide options to deliver wireless into remote areas. See “Wireless Networking in the Developing World,” 2007. <http://wndw.net>.*
2. *Gallup Consulting, “Radio the Chief Medium for News in Sub-Saharan Africa,” June 23, 2008. <http://www.gallup.com/poll/108235/radio-chief-medium-news-sub-Saharan-africa.aspx>.*

3. *Malkhadir M. Muhumed, “Somalia’s Fragile Government Tries to Counter Propaganda Blitz from Militants,” AP Press, March 2, 2010. <http://religion.gaeatimes.com/2010/03/02/somalias-fragile-government-tries-to-counter-propaganda-blitz-from-militants-1347>.*
4. *Jason Straziuso, “Telecoms Accede to Taliban Demand, Stop Cell Service at Night,” AP Press, March 27, 2008. http://articles.sfgate.com/2008-03-27/news/17169253_1_taliban-fighters-zabul-taliban-spokesman.*
5. *Thom Shanker, “U.S. Plans a Mission Against Taliban’s Propaganda,” The New York Times, August 15, 2009. http://www.nytimes.com/2009/08/16/world/asia/16policy.html?_r=1.*
6. *Dawood Azami, “Pakistan’s Taliban Radio Insurgency,” BBC World Service, 22 June 2009. http://news.bbc.co.uk/2/hi/south_asia/8108881.stm.*
7. *The author personally witnessed routine music and news broadcasts in VHF amateur radio bands over Afghanistan in 2002.*
8. *Shanker, Ibid.*
9. *Dictionary.com, retrieved May 1, 2010. <http://dictionary.reference.com/browse/propaganda>.*
10. *Timothy Thomas, “The Age of the New Persuaders” Military Review (May-June 1997), 82-97. <http://www.cgsc.edu/carl/contentdm/home.htm>.*
11. *Muhumed, Ibid.*
12. *Sgt Tracy Smith, “Georgia National Guardsmen Open Radio Stations to Give Afghans Their Own Voice,” WWW.Army.mil, February 4, 2010. <http://www.army.mil/-news/2010/02/04/33958-georgia-national-guardsmen-open-radio-stations-to-give-afghans-their-own-voice>.*



Mr. Lynn Berg is a retired USAF Electronic Warfare Officer who currently works in the areas of electronic warfare(EW) education and training. He served as the Education and Training Branch Chief at the Joint Electronic Warfare Center and has guest instructed on various EW topics at the Naval Postgraduate School, the NATO Staff School in Germany, and the U.S. Army Electronic Warfare Schoolhouse. Mr. Berg completed Air Command and Staff College, the Joint Warfighter’s Course at Joint Forces Staff College, and has a Masters degree in International Relations.



IO SPHERE CALL FOR ARTICLES ON IO INTELLEGEENCE INTEGRATION

IOII

jiowc.iosphere@us.af.mil

ALL SUBMISSIONS DUE BY 15 MAY 2012



Protecting Sensitive Emails

By

Mr. Aaron DeVaughn

Joint OPSEC Support Element



Editor's Note: Operations Security, or OPSEC, is a very important aspect of Information Operations. In this short article, Mr. Aaron DeVaughn provides great insight on how to protect unclassified critical information when using electronic mail. For anyone in IO who deals with sensitive information, this is sage advice.

Did you know encrypting emails is an effective OPSEC measure to protect messages from being read by unintended recipients? It's a known fact that business conducted on DOD networks provides opportunities for sensitive information to be read and compromised when not encrypted.

You can identify what sensitive unclassified information requires protection by reviewing your organization and higher headquarters' OPSEC critical information lists. From an OPSEC perspective, critical information is defined as information about friendly (US, allied, and/or coalition) activities, intentions, capabilities, or limitations an adversary seeks in order to gain military, political, diplomatic, economic,

or technological advantage. Such information, if revealed to an adversary prematurely, may prevent or complicate mission accomplishment, reduce mission effectiveness, damage friendly resources or cause loss of life. If you have not been trained or are not aware of this important document, contact your organization's OPSEC point of contact (POC).

Encrypting emails is not new to the DOD. The DOD has long-standing policies directing users when to encrypt emails. These policies apply to all unclassified email sent from DOD-owned, operated or controlled systems or accounts to include desktops, laptops, and personal electronic devices such as BlackBerry devices.

OPSEC surveys conducted by the Joint OPSEC Support Element found that encrypted emails usually fell into one of three categories: individuals did not configure the computer they are using to send encrypted emails, personnel did not know what to encrypt, and personnel did not know how to encrypt. All of these situations can be corrected by commanders/directors with the help of their OPSEC POC and IT staff. Here's how:

1. Get involved and take an active effort to ensure your



US Navy Aviation Supply Technician Using Unclassified Computer for Operations

Source: defenseimagery.mil

organization's computers used to send sensitive emails are properly configured for encryption. In addition, ensure all personnel publish their Public Key Infrastructure (PKI) certificates to the Global Address List.

2. Ensure personnel are trained on what to encrypt and made aware of your higher headquarters' and your organizations critical information lists. Remember, personnel must not encrypt every email message as this can increase the bandwidth of messages and possibly cause a negative effect on DOD networks.

In addition to being aware of your higher headquarters' and organization's critical information lists, include in training and awareness the need for personnel to encrypt:

Controlled Unclassified Information such as:

- Information potentially exempt from disclosure under the Freedom of Information Act that is marked "For Official Use Only."
- Personal Identifiable Information protected by the Privacy Act.
- An individual's health information that is protected under the Health Insurance Portability Accountability Act Information.

Encryption also protects other sensitive information like:

- DOD Unclassified Controlled Nuclear Information.
- Unclassified Technical Data.
- Sensitive Acquisition Information.
- Proprietary Information.
- Foreign Government Information.
- Drug Enforcement Agency Sensitive Information.
- Antiterrorism/Force Protection Information.
- Law Enforcement Sensitive.

3. Personnel must be trained on how to encrypt sensitive unclassified emails. Incorporate encryption training in initial, annual and recurring OPSEC training. An excellent source for additional training for personnel to know how to encrypt emails can be found at http://iase.disa.mil/eta/using_pki/launchpage (using PKI Certificates).

In this information age, we must control and safeguard our sensitive and critical information to maintain our advantage over our adversaries. When we fail to protect this information, we are the weakest link in protecting our own,

others, and our command's critical information. The ultimate goal of OPSEC is increased mission effectiveness. To prevent our adversaries from gaining access to critical information, you must be the strongest link and encrypt sensitive emails. If you would not hand your sensitive emails to the enemy, don't send them unencrypted. Think OPSEC!

Additional information on OPSEC and encrypting emails can be found at <http://www.facebook.com/home.php#/JIOWC.OPSEC.Support> and <http://iase.disa.mil/pki-pke/>.

With the level of compromise of email on unclassified networks, encryption and OPSEC are critical partners when sending email that contains critical information. ●



US Air Force Technical Sergeant Using Laptop To Communicate

Source: defenseimagery.mil

War Control and Electronic “SHI” China’s Electronic Reconnaissance Goals

by

Mr. Timothy Thomas

US Army Foreign Military Studies Office

Editor’s Note: Mr. Timothy Thomas drafted this article in 2009 as part of his work at the Foreign Military Studies Office (FMSO) at Fort Leavenworth Kansas. The FMSO assesses regional military and security issues through open-source media and direct engagement with foreign military and security specialists to advise army leadership on issues of policy and planning critical to the US Army and the wider military community. The views expressed in this report are those of the author and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or the US government. Mr. Thomas is considered an expert in both China’s and Russia’s military capabilities.

Since 2005, several nations, most prominently the United States, have accused the People’s Republic of China of cyber reconnaissance activities and, on occasion, of the cyber theft of both unclassified and sensitive documents. A cyber-reconnaissance mission is usually designed to plant trapdoors or viruses in another nation’s systems in order to monitor them surreptitiously or to activate them in times of crises. Theft is another issue, in that it involves the outright stealing of sensitive plans whether they are equipment designs, war plans, or some other issue of confidentiality.

While it is important to spot these activities, it is equally important to comprehend the theoretical basis behind them. When viewed separately and out of context, these activities appear less threatening than when they are viewed within an integrative purpose and methodology. With knowledge of an action’s theoretical foundation, it is also easier to point to the action’s probable future intent.

Two traditional Chinese military concepts—war control and strategic advantage—are likely underpinnings for these electronic reconnaissance activities. Reconnaissance activities allow a force to prepare properly for a wartime mission while still in peacetime, activities which support the theories of war control and strategic advantage. They allow a distant force to prepare for close combat, much like an electronic puppet master controlling his outstretched electronic strings to open and close enemy vulnerabilities at will.

This article summarizes the Chinese discussion of war control and electronic *shi* and their relation to reconnaissance. Most importantly, the examination allows for the exposure of the potential strategic intent of the Chinese military as it prepares its forces for twenty-first century eventualities.



A People’s Liberation Army Officer Visits a US Destroyer in 2011

Source: defenseimagery.mil

A Few Definitions of War Control

At the 2009 Chinese symposium on Sun Tzu's Art of War held in Beijing, one of the symposium's breakout groups was devoted to the topic of "war control." War control refers to the guidance and management of a war effort. This term is not familiar to many western theorists since the terms "crisis management," "command and control," "superiority," and "shaping" dominate. The intent and implied use of a term such as shaping is to control a process of some type. Thus, the two nations have concepts that are similar but not identical.

The Chinese have been studying the concept of war control for at least a few years. Evidence of this is a 2002 National Defense University Press book titled *War Control*. Author Xiao Tianliang listed seven parts to the book:

- The theory of war control
- The control of history and the heritage of war
- Controlling conditions in time of war
- Mediating war
- Correctly handling and controlling crises
- The flexible and appropriate use of the means of warfare
- The use of war control in China's future¹

A current definition of war control can be found at the website www.laocanmou.net, a military website located in Lanzhou.

It defines war control as "the political director of war, the occurrence, development, scale, intensity, and consequences of deliberate acts of imposing restrictions and constraints."² War control is defined in the 2001 book *The Science of Military Strategy* as the war conductor's behavior to limit and consciously restrain the occurrence, development, scale, intensity, and outcome of war.³ Thus, the Lanzhou and book definitions are nearly identical, meaning the definition has not changed much over the past several years.

War control involves preventing war, controlling its occurrence, controlling its vertical and horizontal escalation, and striving to reduce the consequences of war. The essence of war control is the strategic conductor's initiative in controlling and mastering war. National interests should strictly control military strength. The selection of war means must correspond with the object of interest to be obtained, and the war's conductor should adjust military strategy according to the national interests at stake.⁴

Arms control, crisis control, and armed conflict control are all components of war control.⁵ Arms control is divided into vertical arms control and horizontal arms control, with the former aimed at limiting or reducing the scope of military potential and the latter aimed at limiting the proliferation of certain weapons.⁶ Crisis control is control of the tense political and military situations caused by intensified contradictions of national interests; i.e., one must strive to remove the negative factors leading to a crisis. A crisis is a dynamic process, and it includes the stages of inception, escalation, de-escalation, and termination. The measures for crisis control



Former Chairman of the Joint Chiefs of Staff Admiral Michael Mullen Speaks with the Media After a Joint US and China Military Band Music Concert

Source: defenseimagery.mil

and management are confidence-building (measures to prevent the emergence of a crisis), increased transparency, enhanced personnel exchanges and contacts, joint disarmament and arms control, the establishment of regulations, and the creation of supervisory organizations.⁷ To control a crisis, one must find the intersection of interests, compromise appropriately, and strive for benefit for both sides, keep uninterrupted communications, and adopt coercive measures to prevent negative influences (weapon embargos, economic sanctions, and military blockades).⁸ The control of armed conflict includes the control of its aim, means, targets, methods, duration, and space of the conflict.⁹

Peng Guangqian and Yao Youzhi, the editors of *The Science of Military Strategy*, write that the essence of war control is the strategic conductor's initiative in controlling war. The strategic conductor must give play to his subjective initiative and carry out correctly strategic guidance to prevent the occurrence of crises and the escalation of a conflict. Only in this way can the objective of war control be attained. National interests are the guiding element in war control and strategic conductors must grasp national

interests in a fundamental, long-term sense. These interests control military strength and the war means to be used.¹⁰

The preparation stage of war control is where reconnaissance enters the equation. This includes scientific predictions on the prospects for war or crises. Plans to cope with crises and contingencies must be arranged in peacetime. The preparation of military strength is the essential and most reliable preparation for all war control events. Non-military means must also be employed, to include the preparation of economic means as the foundation, political means as the dominator of all events, and military means as the backup force. War control can only be achieved when these comprehensive military and non-military means are prepared.¹¹

Finally, war control involves observing and applying international law. Any strategic war control conductor must take these laws into consideration in their planning process.¹²

Definitions Offered at the Symposium

Several opinions were offered on war control at the breakout session of the Sun Tzu Art of War symposium. First,

a Taiwanese representative opined that there were three aspects of war control: prevention, controlling the scale and depth of a war, and reducing risk after war breaks out. He focused his attention thereafter on the prevention aspect. He noted that prevention also has three aspects. The first is the control of "slope theory," or the ability to keep war from sliding into an abyss from which no one can escape. Sometimes third parties on the fringe are needed to stop two other parties from sliding down a slippery war slope. A second aspect is constructing a smooth channel of information so that communication is never cut off. If a channel of communication or information is cut off, then miscalculations will result. Finally, when a party feels threatened or stepped upon, there must be a correct way to find an outlet to express this perceived misrepresentation of justice. If not, then war will occur. The Taiwanese representative felt this is what occurred on 9/11 with Bin Laden, that he had no other recourse or outlet to express his rage. Most Americans would obviously disagree with this assessment.

A Chinese military officer from the Academy of Military Science at the Sun Tzu symposium offered three phases



PRC Sailors in Formal Uniform
Source: US Navy

to war control. They were preventing or dissolving a crisis, controlling the war process (that is, its magnitude and scale), and controlling a war's outcome. Subordinate tasks include controlling a conflict's escalation and controlling miscalculations.

War Engineering—The Information-Age Version of War Control?

There is another concept under consideration by the Chinese military that is similar to war control: the concept of war engineering. Major General Hu Xiaofeng, a professor in the Information Operations and Command Training-Teaching and Research Department at China's National Defense University, noted that the age of informatization requires new approaches to the study and management of information-age wars. War engineering is one of these new approaches.¹³

War engineering arose, Hu contends, from the requirement to find a method to study, manage, and control information-age

war systems. Chinese war engineering is "a method of systems engineering that studies, designs, tests, controls, and evaluates war systems and that is guided by systematic thinking, based on information technology."¹⁴ The most important element of war engineering is to maintain control of war systems. Through war systems, control of the course of operations is possible.¹⁵ The concept is centered on managing warfare and has total victory as its goal.

War engineering looks at combat as a nonlinear, complex adaptive system. War engineering studies, designs, and manages war requirements, theories, experiments, and processes. It has five parts: requirements, planning, testing, control, and evaluation engineering. Control engineering, the most important element, consists of strategic, campaign, and tactical command information systems which monitor situations, control decision-making, handle anomalies, and evaluate results.¹⁶

Hu concludes his thoughts on war engineering by quoting Engels, who

noted that "it wasn't the inventors of new material measures; it was the first person who, in the correct manner, used a new measure that had already been invented." Hu believes China is searching for a way to be the first to use US information-age inventions to their benefit and prove Engels correct. China hopes to be able to manage and control war instead of reacting to it and to make wartime changes in advance (through simulations) instead of making changes as war requires or demands. War engineering, according to Hu, will be one of several catalysts that promote the further development of information war studies as China transforms its military from a mechanized to an informatized force.¹⁷

The term war engineering was brought to the attention of the Sun Tzu war control panel and its moderator. The Chinese participants were asked if war engineering and war control were the same thing. The moderator stated that not much importance should be attributed to the term since it appeared in the journal *China Military Science*. The journal, he



Senior PLA and PRC Navy Officers Pose for Photo During Official Visit Aboard US Vessel

Source: defenseimagery.mil

noted, is a place for new ideas and not policy. However, the discussion of the term clearly indicates that war engineering and war control are two ideas from the same cut of cloth.

Electronic *Shi*

Shi is an important strategic Chinese concept with roots as far back as Sun Tzu's classic *The Art of War*. One US source defines *shi* as the strategic configuration of power or advantage.¹⁸ A retired Chinese General, Tao Hanzhang, defines *shi* as "the strategically advantageous posture before a battle that enables it to have a flexible, mobile, and changeable position during a campaign."¹⁹ Another Chinese source, the book *Campaign Stratagems*, defines *shi* as the combination of the friendly situation, enemy situation, and the environment as the sum of all factors impacting the performance of the operational efficiency of both sides and as the key factor determining the rise and fall of operational efficiency.²⁰

The term *shi* (pronounced like the English word "sure") appears 80 or more times in Chinese dictionaries and each time it is expressed by a different Chinese character with a different meaning (but is pronounced the same except for stress).²¹ *Shi* (as is the case with many Chinese pinyin expressions) can be expressed linguistically via four tones, which are: neutral, ascending, descending, or descending-ascending. For each tone there are twenty or so different Chinese characters. For example, the words ten, teacher, non-commissioned officer, time of day, to begin, to be, to test, to make, to see, to know, room, and thing are all pronounced via one of the four tones of *shi*. Each one is expressed/written with a different Chinese character. Therefore it is important to know just which Chinese character of *shi* one is speaking about and defining. In the case for this article, we are using the *shi* character for strategic advantage.

Electronic *shi*, then, is the attainment of an electronic strategic advantage. United States defense officials recognize Chinese attempts to realize electronic *shi* in today's digital environment. The US Deputy Undersecretary of Defense for Asia-Pacific affairs, Richard Lawless, told Congress in 2007 that the Chinese military's "determination to familiarize themselves and dominate to some degree Internet capabilities—not only of China and that region of the world—provide them with a growing and very impressive capability that we are very mindful of and are spending a lot of time watching."²² The attainment of a strategic advantage enables control.

The apparent goal of the People's Liberation Army (PLA) newly-developed digital prowess/quantum leap is to allow it to be fully prepared to achieve electronic *shi* early in the twenty-first century. An electronic advantage could be attained by uncovering vulnerabilities in a potential enemy's digital systems through reconnaissance activities or by planting computer viruses in such systems. Both activities would occur in peacetime and both activities would allow the PLA to gain an initial advantage if war broke out. Only with electronic *shi* can the PLA "win victory before the first battle." Achieving such advantages requires updating the PLA's thinking with informatized modes of thought.

Conclusion

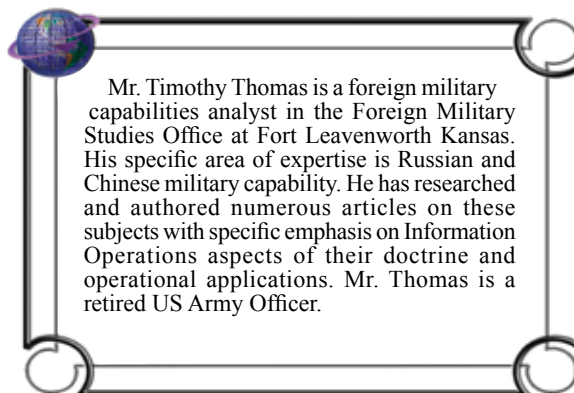
The topics of war control and electronic *shi* are foreign to US audiences. However, the former is a topic of immediate concern and extended discussion in the People's Republic of China (PRC) and the latter is the former's probable extended goal. It is important for western audiences to become familiar with these and several other Chinese theoretical topics if they are to comprehend what is behind the extended military and civilian

reconnaissance efforts of the Chinese. Viewed separately and out of context, they are less threatening than when viewed within an integrative purpose and methodology.

Successful electronic reconnaissance activities enable the PLA to put into place the initial stages of their war control planning process. Such activities also provide electronic *shi* or electronic strategic advantage at the start of any conflict. Western analysts must become aware of the purpose behind Chinese reconnaissance activities instead of merely assuming the PLA is stealing information. According to their theory, they are doing much more than that. ●

Endnotes:

1. Book description found at www.bi3jia.com, accessed 10 November 2009.
2. Website and translation provided to the author by Mr. Scott Henderson, FMSO, on 10 November 2009.
3. Peng Guangqian and Yao Youzhi, *The Science of Military Strategy*, Military Science Publishing House, 2005. The section on war control was reprinted as an article in the journal *China Military Science*. See "War Control," *China Military Science*, Number 6, 2005, pp. 129-141, in English.
4. Peng and Yao, p. 209.
5. *Ibid.*, p. 197.
6. *Ibid.*, pp. 199-200.
7. *Ibid.*, pp. 202-204.
8. *Ibid.*, pp. 205-206.
9. *Ibid.*, pp. 207-208.
10. *War Control*, p. 139.
11. *Ibid.*, p. 140.
12. *Ibid.*, p. 141.
13. Hu Xiaofeng, "The Basics of War Engineering," *Beijing Zhongguo Junshi Kexue (China Military Science)*, No. 3, 2007.
14. *Ibid.*
15. *Ibid.*
16. *Ibid.*
17. *Ibid.*
18. Ralph Sawyer, *The Art of War*, Fall River Press, 1994, pp. 143-147.
19. Tao Hanzhang, *Sun Tzu's Art of War: The Modern Chinese Interpretation*, Sterling Innovation, 2007, p. 124.
20. Zhang Xing Ye and Zhang Zhan Li, editors, *Campaign Stratagems*, National Defense University, 2002, pp. 8-18.
21. Discussion with Chinese language instructors Marn-Ling Wang and David Dai at the US Defense Language Institute, July 2009.
22. John Tkacik, *Trojan Dragons: China's International Cyber Warriors*, WebMemo, 2007.



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 including core, supporting and related capabilities, as well as 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 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

TO SUBSCRIBE: If you or your organization would like a free subscription to *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 copies requested. 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. Finally, 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 Electronic Warfare, Public Affairs, Strategic Communication, Military Information Support Operations, IO Education and Training, IO Intelligence Integration, and IO Support to Public Diplomacy.



IO SPHERE: SUBSCRIPTION 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? _____ No. Copies (3 Max): _____

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? _____

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

Under "lists" click "IO Sphere Subscription"

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



"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