

May 2012

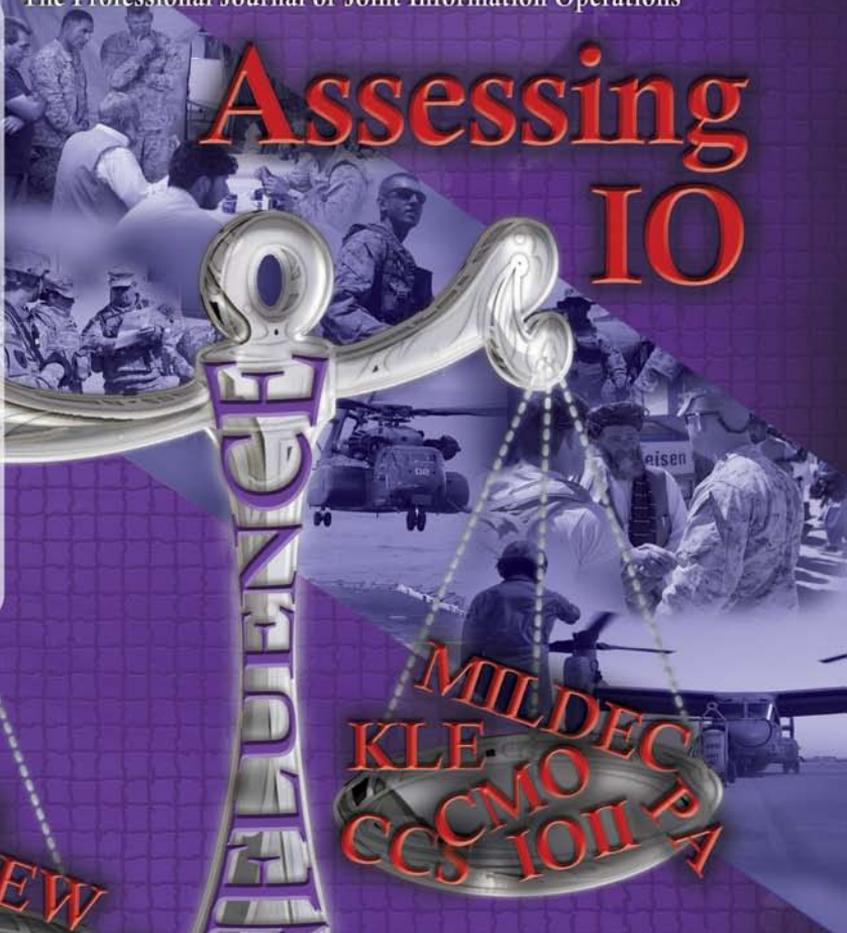
IS PHERE

The Professional Journal of Joint Information Operations

IN THIS ISSUE

- Assessing IO
Brig Gen John N.T. Shanahan.....Pg 2
- Best Practices
Mr. Bruce Judisch.....Pg 4
- Joint Information Operations Assessment
Mr. Charles Chenoweth.....Pg 10
- Assessing COIN Information Operations
Dr. Stephen Downes-Martin.....Pg 16
- Information Environment Training
and Education
COL Carmine Cicalese.....Pg 22
- JIOWC Transregional Conflict Prevention
Initiative (TCPI)
Mr. Richard Josten.....Pg 27
- Change of Leadership at the US Marine
Corps IO Center.....Pg 33
- A Match Made in Cyberspace
LTC Gerald R. Scott.....Pg 34

Assessing IO



CNO STO
MISO EW
OPSEC

MILDEC
KLE
CCS CMO
IOII PA



Joint Information Operations Warfare Center

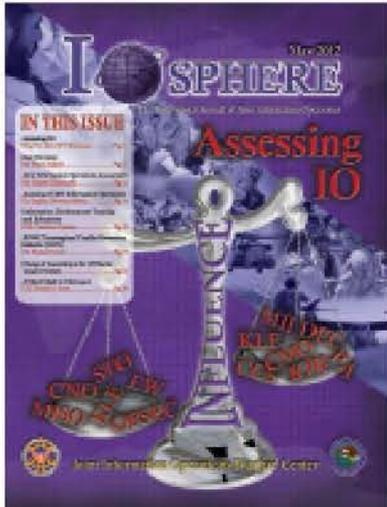




IO SPHERE

FEATURE ITEMS and ARTICLES

Assessing IO	
John N.T. Shanahan, Brigadier General US Air Force	2
Best Practices: Thoughts and Perspectives	
Mr. Bruce Judisch	4
Joint Information Operations Assessment Methodology	
Mr. Charles Chenoweth	10
Assessing COIN Information Operations Aimed at the Local Population	
Dr. Stephen Downes-Martin	16
Information Environment Training and Education Considerations for the Joint Force 2020	
Colonel Carmine Cicalese, US Army	22
JIOWC Transregional Conflict Prevention Initiative (TCPI)	
Mr. Richard Josten, Department of the Air Force Civilian	27
Change of Leadership at the US Marine Corps IO Center	33
A Match Made in Cyberspace: Secure Function Evaluation in Military Planning	
Lieutenant Colonel Gerald R. Scott, US Army	34



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 Services Inc. and the JIOWC.

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

About the Covers: The front and back cover represent the various aspects of global reach and operations involving Information-Related Activities.

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

IO Sphere Key Staff

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

Mr. Henry (Keith) Howerton
 Editor and Layout Design
 Webhead Inc
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 SIPRNet 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 .mil official domains CAC credentials are required.

Corrections and Retractions

In the December 2011 Issue of *IO Sphere*, an article by Major Jay Anson on US Army IO contained references to Army IO doctrine that is dated. At the time Major Anson wrote the article, he was referring to the most up to date doctrine available. The doctrine changed after he authored the article.



Civil Military Operations

US Marine mixes cement while building school in US Southern Command Area of Operations.

GENERAL SUBMISSION GUIDELINES:

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

TEXT - Microsoft Word.

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

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

FORMAT/LENGTH - 500 words or more double spaced.

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

jiowc.iosphere@us.af.mil
Or

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

CALL FOR ARTICLES

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

Disclaimer Statement

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

Assessing IO

By

Brig Gen John N.T. Shanahan

Deputy Director for Global Operations

Joint Staff J-39

Recent public media reports and congressional inquiries have once again highlighted the need for the IO community to provide meaningful assessments of DOD information-related activities. When combined with the long-standing requirement of commanders at every level to be able to assess the contribution of IO to a single operation or an entire campaign, it is imperative now more than ever that we quantify the return on investment of information-related capabilities. We must demonstrate both *impact* and *value*. As I noted in my remarks in the previous issue of *IO Sphere*, in an era of shrinking budgets the phrase ‘survival of the fittest’ comes to mind—those programs that cannot demonstrate the value of their contributions risk an ignominious ending at the sharp end of the budget guillotine.

IO assessment is difficult, but not impossible. There are a variety of initiatives underway in OSD Policy and on the Joint Staff, with the goal of creating a process that delivers insightful and metric-driven assessment data. If these efforts bear fruit, as I fully expect they will do, there will be a major impact on the IO enterprise for years to come. Regardless if we call it an assessment process, an assessment framework, or some other term, a concerted team effort is essential to align ends, ways, means, risks, and resources to ensure the warfighter has the tools to determine the value of IO to mission accomplishment.

The goal of assessing IO is to analyze the performance and effectiveness of integrating and employing Information Related Capabilities (IRC). This methodology must provide feedback, uncover shortfalls, identify policy and resource



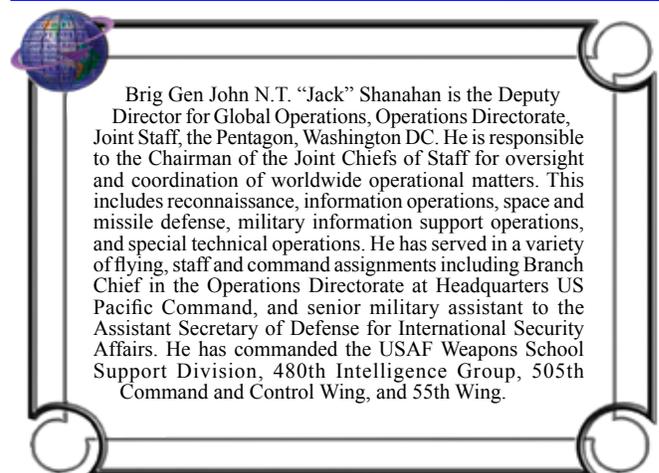
challenges, and ultimately provide relevant information that captures return on investment. Absent a user-friendly IO assessment and feedback loop, we will continue to grapple with how to demonstrate value added to the DOD mission.

As IO professionals, we know we have an impact that is often evaluated more by what we do than by any immediate revelation of effects we might have had. Additionally, it can be extremely difficult to show what the results may have been had we *not* conducted the information-related activity in the first place (the counter-factual argument). In the past, it is fair to say that too often we were able to get away with an approach that focused almost exclusively on funds expended and activities performed or, in even simpler terms, the “we spent a lot of money and here are all the great things we did” mantra. When funding begins to dry up, that philosophy is a recipe for extinction.

It is often too easy to ignore the requirement for assessment of IRCs, falling back on the somewhat glib proclamation that “IO effects take years to manifest themselves.” There is unquestionable truth to that statement, as results associated with trying to change attitudes and perceptions might take decades to be revealed, if it ever happens at all. Yet this is no excuse for ignoring the need to focus on metrics. Metrics provide the starting point for IO assessment. We must improve methods of collecting and capturing relevant data, and then accurately translate that data into measurable results. This edition of *IO Sphere* includes the first of several articles on an IO assessment framework. It is an excellent starting point. The Joint Staff J-39 IO and MISO Divisions and others at the policy-making level, as well as the IO community at large, already have begun working the problem in earnest. We need the support of the entire IO community to keep advancing the assessment cause.

As we enter an era of austerity with increasing scrutiny of how money is expended, I solicit your participation and good ideas to improve our ability to measure the return on investment for IO and highlight how it can and should be a force multiplier. When running away from the bear, while it’s true that to survive you only have to run faster than the person running beside you, if you are slower than your companion it helps immensely to convince the bear that your survival is value added to the bear’s existence. Help us figure out not only how to run faster, but also to convince the budget grizzly that properly applied IO is exactly what we need more of, when the rest of the big-ticket kinetic force is faced with hard times ahead. ●

Brig Gen Shanahan



JOINT INFORMATION OPERATIONS PLANNERS COURSE



Joint Forces Staff College

Only DOD Certification Course for Joint IO Planners

DOD Requirement for Joint IO Planning Billets

Earn College Credits



MISO
CNO
MILDEC
EW
OPSEC



Public Affairs
Defense Support to
Public Diplomacy
CMO

Physical Attack
IA
Physical Security
CI
Combat Camera

Visit our Website
www.jfsc.ndu.edu

Learn About

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

Graduates Will

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

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

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

Best Practices: Thoughts and Perspectives

By

Mr. Bruce Judisch

Editor's Note: Mr. Judisch's essay on "Best Practices" has a direct impact and correlation in assessing the impact of IO. In reality there is no way to discover a best practice in any field of study or profession without first conducting a comprehensive and detailed assessment of the focus area. It is for this reason that his contribution to this issue of *IO Sphere* is so important.

"Excellence is an art won by training and habituation.... We are what we repeatedly do. Excellence, then, is not an act but a habit." - Aristotle

Best practices are in fact little more than excellence with broad applicability. Excellence refined through Aristotelian habit appears in a wide variety of contexts in nearly every enterprise, whether academic or industrial, public or private. Indeed, the impetus to highlight and adopt such practices is neither complicated nor new. St. Paul grasped its essence when he exhorted the church at Thessalonica to "prove all things; hold fast that which is good."¹

In the best-practices arena, holding fast to that which is good is taken a step further in adopting that which is good across a span of kindred operations. Of course, this seems reasonable. Who could argue? Yet, as intuitively good as it may seem, the concept of best practices is not without its critics.

If Not, Then What?

Contextual Practices

One such critic is Scott W. Ambler, Chief Methodologist for Agile and Lean at IBM Rational, who addresses best practices

"Calling something a 'best practice' implies that it's a good idea all of the time, something we inherently know to be false."

in software development. He argues, "Ideally, we shouldn't talk about best practices at all but instead should talk about contextual practices. Depending on the context, sometimes a practice is 'best' and sometimes it's not. Calling something a 'best practice' implies that it's a good idea all of the time, something we inherently know to be false." He adds, somewhat tongue-in-cheek, "Having said that, the term 'best practice' clearly has more marketing value than the term 'contextual practice', and in this industry we know that marketing typically wins over truth, something that is clearly not a best practice."²

As the name implies, a contextual practice derives validity and value from the context in which it's applied. The more contexts it fits, the closer to the traditional broad-scope best practice it becomes. What Mr. Ambler implies is that it won't apply as-is across the enterprise as a one size fits all. Therefore, those who do adopt it retain the right to modify it, as appropriate.

Smart Practices

Eugene Bardach, Professor of Public Policy, Emeritus, at the University of California's Goldman School of Public Policy, champions another alternative: smart practices. These are similar in essence to contextual practices. The focus here, though, is upon their derivation, which is based primarily upon organic cost-benefit analysis. In his contribution to *Innovations in Government: Research, Recognition and Replication*, Dr. Bardach writes, "By smart practice I mean a practice that takes advantage of some latent potentiality in the world in order to



US Riverine Sailors Discuss Best Practices with Royal Brunei Navy Support Squadron Sailors

Source: defenseimagery.mil

accomplish something in a relatively cost-effective manner.... To put it another way, smart practices are smart because they exploit some latent potential [of the environment] to get a lot of bang for the buck.”³

The thought here is that a given environment not only validates a practice, but actually feeds the practice; i.e., participates in its action.⁴ Such an approach further individualizes these practices, turning the focus on their individual attributes within a scenario rather than their applicability across several scenarios (i.e., depth vs. breadth). The task then becomes one of comparing those attributes for commonalities and devising practices to either influence the environment or operate effectively within it. Inevitably, the result will be the same as we saw with contextual practices: because the individual scenarios carry elements uniquely their own, the practices they engender will do likewise, and therefore will largely negate the possibility of an enterprise-wide, shrink-wrapped application.

Other Terms

Attempts to grapple with the best-practices problem elsewhere in public service and in private industry have yielded terms such as “promising practices” and “evidence-based practices.”⁵ To an extent, these confuse—or perhaps merely reflect confusion in—the analysis and implementation of concepts wanting to be known as best practices. Analysis

and comparison of these terms reveal that reticence to accept the superlative ‘best’ qualifier appears to be due to its universal-remedy connotation, whether that impression is completely fair or not.

The Problem Applied

Best practices are an output of lessons learned, a discipline governed in the Department of Defense (DOD) by the CJCSI/M 3150.25 series. The joint community defines it as “A non-doctrinal tactic, technique, or procedure that is in current field use and appears to be potentially worthy of replication.”⁶ The manual goes on to say, “All best practices should be critically considered in light of the local situation and capabilities prior to implementation. A validated best practice may eventually lead to an issue for DOTMLPF⁷ resolution.”⁸ This is good in that it stops short of mandating an *a priori* enterprise-wide duplication of the practice, rather simply credits it with some level of success and deems it potentially worthy of replication. In this sense, it fits the description of Mr. Ambler’s “contextual practice.” However, the begged question is whether a given practice solves similar problems or enhances operations in other contexts, thereby obviating the need to reinvent the wheel multiple times. From that perspective, the contextual practice invites the rigor needed to qualify, tailor and adapt it into other scenarios. This process could entail Dr. Bardach’s cost-benefit approach, a functional feasibility assessment, an organizational profiling

to determine whether the practice fits within the force construct necessitated by the tactical problem—or a combination of these and other measurements. Rarely will it be plug-and-play out of the box, as appealing as that prospect might be to the time-constrained and resource-strapped IO integrator, planner or operator.

Such constraining and strapping acknowledged, operational success disallows austerity in materiel resources or time to rule the day; it is still a best practice and is therefore worthy of evaluating for replication. We can afford neither to reject a recommended practice out of hand as a hastily perceived misfit, nor arbitrarily attempt to cram someone else’s round solution into our square problem. Due diligence lies somewhere in between.

The Nature of the Best

Like taffy, the broader the scope a practice is stretched to fit, the thinner it tends to become.

The problem is not recognizing and isolating practices,⁹ it’s retrieving them from isolation, tailoring them for common adoption, and even improving upon them for sustained applicability into the future. It is also recognizing their bona fide applicability to similar operational environments and, as already noted, applying the analytical rigor needed to validate and modify them to whatever extent needed.



US Marine Corps Officer from Marine Forces Pacific Share Best Practices with Asian Allied Partners

Source: defenseimagery.mil

Like taffy, the broader the scope a practice is stretched to fit, the thinner it tends to become. Practices observed and insights gleaned at levels that apply most widely across operations in multiple areas of responsibility (AOR) often court the tendency to read like generally accepted principles of leadership/management; e.g., optimize span of control, flatten the organization's hierarchical profile, empower those at the appropriate levels of leadership, decentralize execution. Good professional military education (PME) reminders, but shallow terrain from which to mine nuggets of sufficient value to stimulate change downrange. The problem for the IO "best practitioner" is that cross-AOR applicability seems to decrease proportionately with the echelon of command, as operations become more scenario/environment oriented with respect to such diverse factors as target-audience demographics (density, accessibility), cultural nuances (language, mores), and degrees of technological maturity and access.

For example, Joint Staff J-7, as the joint entity responsible for lessons learned and best practices, publishes an excellent journal, *Joint Operations Insights & Best Practices (I&BP)*.¹⁰ Smaller pamphlets, titled *Insights & Best Practices Focus Papers*, aperiodically cover single topics between releases of their more comprehensive parent journal. The third edition of *I&BP*, issued in January, 2011, compiled observations of exercises and real-world operations over a two-year period, leading to numerous recommendations at various levels of command. Most of the insights residing at the upper echelons of command (at the multinational/coalition level through combatant commands to joint task forces) resemble the PME reminders mentioned earlier. Under subjects like "Command-centric Leadership" and "Command and Control," the journal enumerated such advisements as to give subordinates credit when due, accept responsibility when things go poorly, maintain a broad perspective, provide definitive guidance but don't micromanage, and the like.¹¹ And this is not a criticism; these are proper and valid advisements worthy of the ink and paper they consume. They're also generic enough to fit neatly into a management curriculum at any public or private organization.

To be fair, more specific methods of operation are noted; however, they often appear as insights, not practices. For

example, *I&BP Edition 3*, under the general heading of "Command and Control," sub-heading Task Organization, offers insights on the way geographic combatant commands (GCC) organize subordinate functions:

*"For smaller contingencies, we're seeing the GCCs establishing subordinate JTFs with focused missions and geographic-oriented JOA. For larger GCC-controlled operations, we're seeing the GCC use of traditional functional components (i.e., JFLCC and JFMCC) being given AOs. We've even seen in some cases the JFACC and the JFSOCC being given AOs. At the JTF level in land-centric operations we've seen geographically-based organizations..."*¹²

Insights, remember, are discernments of the nature of something, whereas a practice is the performance or application of an insight. The above example is a statement of what is, not an advocacy of what should be.

Regardless of its nature, the value of the practice is discerned through a controlled process, or methodology, after which it is ultimately either adopted as "best," or discarded altogether.

Methodology

Ironically, there's no best practice in formulating best practices. As one would expect, best-practice discovery, analysis and implementation methodologies vary with industry, and within each industry according to the problem sets against which they're applied. Constraints and restraints—time, resources, and performance expectations—dictate the type and amount of attention that can be afforded this discipline. For example, some processes employ a hierarchical system that progressively qualifies a practice on its way to become 'best'. Others feature a cyclic element, revisiting and reevaluating those practices adopted as best on a periodic schedule to ensure currency as the problem set, or operational environment, evolves. Borrowing from the public sector once again, the healthcare industry uses a three-tier hierarchy of practices, each qualified by a more thorough level of evaluation. They're recapped below in ascending order of maturity.

Hierarchical - Three Tiers of Practices¹³

Research-Validated Best Practice	A program, activity or strategy that has the highest degree of proven effectiveness supported by objective and comprehensive research and evaluation.
Field-Tested Best Practice	A program, activity or strategy that has been shown to work effectively and produce successful outcomes and is supported to some degree by subjective and objective data sources.
Promising Practice	A program, activity or strategy that has worked within one organization and shows promise during its early stages for becoming a best practice with long term sustainable impact. A promising practice must have some objective basis for claiming effectiveness and must have the potential for replication among other organizations.

Here a practice evolves from coal to diamond, but with design.¹⁴ The “promising practice” carries as part of its definition the potential for becoming a “best practice.” That potential then undergoes empirical scrutiny before its promise is realized.

Another example, this one from the energy trade, segments best practices by profit-loss functions, as the organizational constructs within the industry tend to be arranged (e.g., nuclear, renewable, oil & gas, energy management). In one giant of the industry, the practices are discerned, evaluated, approved and implemented according to a tight, rigorous process. They are then centrally validated and approved, and, after implementation, undergo periodic reevaluation to ensure sustained relevance, or currency. This process is duplicated in parallel between the functional segments of the organization.

In the joint military context, a similar construct exists, but with some differences. The Joint Lessons Learned Program (JLLP) delineates four steps in the lifecycle of a lesson learned, which may yield a best practice.

The Joint Lessons Learned Program Four-Step Process¹⁵

Discovery: Initial phase of gleaning unrefined information for consideration from multiple sources; e.g., early observations, first impressions, preliminary reports, significant events, incidents or activities.

Validation: Formal review of raw data to convert observations into findings, ensuring completeness, functional relevance, credibility, and applicability. Upon validation, the information is considered a lesson, which can be either a finding, an issue, a recommendation, or a best practice.

Integration: Forwarding lessons to the learning and functional issue-resolution processes for review and integration; e.g., incorporation into joint and service doctrine, and training & education processes.

Evaluation: Determining the effectiveness of the practice to enhance operations or redress shortfalls, and whether it is worthy of sustainment and improvement. After passing this phase, the practice is either identified for further work, or readied for publishing and disseminating to the community of practice.

This methodology is depicted in Figure 2 (page 8) in a process-flow format and is best described in the following way.

Discovery: The Birth of the Best

Insights and best practices are gleaned in a variety of settings. Here, a best practice is spawned as an observation, a practice that is “...unrefined and not validated but is under consideration for additional review and analysis.”¹⁶

Observations are produced from both active collection (i.e., sponsoring specific events to generate observations, such as exercises and experiments) and passive collection (i.e., leveraging lessons learned from external or after-action sources). In the healthcare model cited above, observations at this point of development would be called promising practices; in Mr. Ambler’s software-development world, contextual practices.

Such observations are best-practice diamonds in the rough. And, like any gem worth setting, they must transit multiple stages of maturity in pursuit of excellence, requiring the heat and pressure of scrutiny and refinement to realize their ultimate integrative worth. We noted that the healthcare industry tags the practice through the three stages of its lifecycle. The joint community focuses more on the stepped process to mature the observation to a practice.

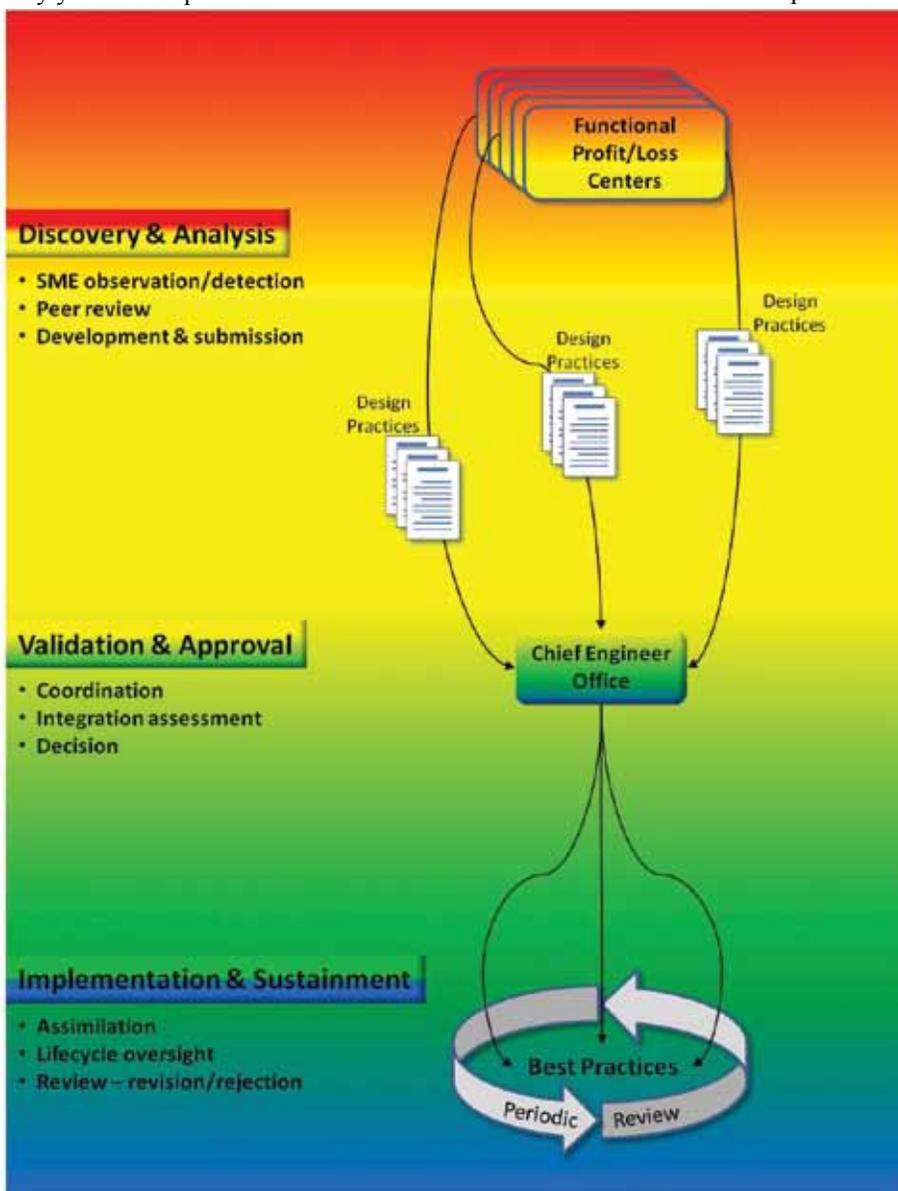


Figure 1. Central Approval and Periodic Review

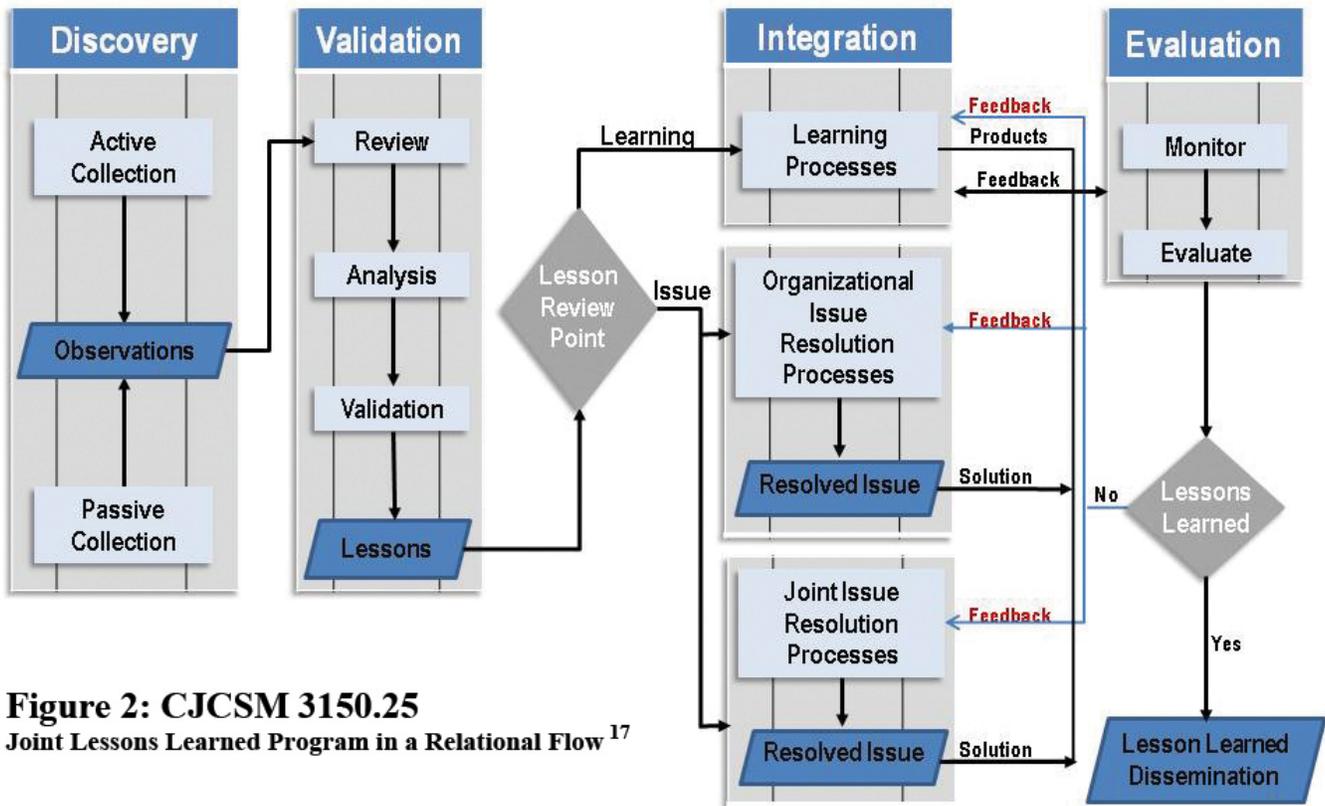


Figure 2: CJCSM 3150.25
Joint Lessons Learned Program in a Relational Flow¹⁷

Attempting to socialize what has been deemed as a best practice is the rub, and it's often the point at which it draws its final breath.

Validation: The Growth of the Best

This second phase comprises four steps: analysis, review, validation, and release.¹⁸ It consists of “analytic and review activities necessary to convert observations into validated findings.”¹⁹ Applied empirical rigor with respect to both depth (applicability to the current context) and breadth (integrative potential) should either disqualify the practice, or refine it. That said, the actual JLLP analysis phase is not standardized, but rather is highly subjective; that is, it exhibits more flexibility than rigor. Those potential best practices that survive to implementation, do so through vested championing, not necessarily by virtue of any self-evident value.

However, pronouncing a practice as being “best” often merely props it up with a bull’s eye painted on its chest. There remains the task of socializing the practice, gaining acceptance, and implementing it into indigenous operations, all within a context of varying degrees of skepticism on the part of the operational community.

Integration and Evaluation: The Best Matured

Attempting to socialize what has been deemed as a best practice is the rub, and it’s often the point at which it draws its final breath.²⁰ Given Mr. Ambler’s assertion that it’s intuitively obvious no practice is the right practice for all circumstances, how does a practice gain general acceptance as being best? Perhaps the answer to his point is that it doesn’t have to be right for all circumstances, just for as many as possible. In the joint community, highlighting observations for common consideration is facilitated by the Joint Lessons Learned Information System (JLLIS).²¹ However, JLLIS mandates neither acceptance nor implementation of a best practice—it’s merely a knowledge-management system; that is, the tool simply tracks the practice through its lifecycle, however long that may be. That lack of authoritative leverage leaves the practice suspended in space, fruit for the picking at the market’s discretion. And the fruit that is not picked is too often left to rot, re-seed, then sprout elsewhere requiring it to be re-harvested yet again.

So What?

There appears to be genuine differences of opinion across industries regarding both the nature and the value of best

practices, regardless of how they’re labeled. Yet, to an extent, all industries employ some semblance of the concept through, if nothing else, common-sense efficiency measures. That is, there may or may not be a formal process, but learning from ours and others’ mistakes—and successes—is essential as much for commercial as for personal survival. This fact alone lends sufficient importance to identifying, analyzing and implementing best practices.

Operational survival being no less important than commercial and personal survival, it’s intuitive that learning from ours and others’ successes and failures at the strategic, operational and tactical levels is an equally worthy endeavor. DOD has embraced a formal process to accomplish this and has codified it, thereby recognizing its value. Yet, despite DOD’s endorsement, challenges remain in socializing what emerges from a sometimes laborious JLLP and resides in an often-viewed cumbersome JLLIS. To that end, perhaps it’s advisable to view best practices through lenses that see beyond the formal JLLP. No process or tool should become an albatross around the neck of an excellent idea. Excellent practices continue to surface at all levels, yet many are condemned to an endless cycle of reincarnation as personnel rotate and continuity is lost. The question is, if

not through the JLLP, then how can excellence be propagated without stove-piping or fragmenting the effort? Simply trading the ‘lessons learned’ moniker for a euphemism will quickly betray its own transparency, showing a lack of any substance to sustain it.

Socializing excellent ideas requires leadership buy-in, but is only fully realized at the point of impact: the analytical team, the planning cell, boots on the ground. The greatest obstacle to that socialization is inertia, here birthed by a dynamic operational environment and nurtured by steadily dwindling resources. Generating sufficient motivation to overcome this inertia ultimately requires the determined energy of the entire organization. Best practices, evaluated and tailored to suit, benefit the whole—either directly or indirectly—and they need to be embraced by the whole. That truth may well require reforming the popular perception of JLLP/JLLIS, or retooling them into a more popularly accepted mechanism for embedding improvements into the field. How to accomplish such a task is a lesson worth learning. ●

Endnotes:

1. *Thessalonians 5:21 (KJV)*. Although directed to the Thessalonian congregation in the context of discerning doctrine, such epistles were normally circular, and Paul most certainly extended this axiom as a “best practice” across the enterprise of the early Christian church.
2. Scott W. Ambler, “Questioning “Best Practices” for Software Development”, <http://www.ambysoft.com/essays/bestPractices.html#ContextualPractices>
3. Eugene Bardach, “Developmental Processes: A Conceptual Exploration,” *Innovations in Government: Research, Recognition, and Replication*, (2008): 130-131. This is a professional journal sponsored by the Ash Institute for Democratic Governance and Innovation, and published by the Brookings Institute Press.
4. As an example in the physical world, Dr. Bardach offers, “...a seagull taking advantage of gravity to open a shell by dropping it on a rock, or a human being exploding some energy-packed hydrocarbon molecules in an enclosed chamber in order to move a two-ton truck.” In an example closer to the heart of the IO planner, he suggests, “In the social world...we take advantage of easily induced fear and uncertainty to deter unwanted behavior...” (Bardach, 131)
5. “Evidence-based practices” are used within the health-care industry interchangeably with best practices. The phrase denotes “...the conscientious use of current best evidence in making decisions about the care of individual patients or the delivery of health services. Current best evidence is up-to-date information from relevant, valid research...” (<http://www.cochrane.org/about-us/evidence-based-health-care>)

6. *CJCSM 3150.25, Joint Lessons Learned Program, 15 February 2011.*
7. *Doctrine, organization, materiel, leadership and education, personnel, and facilities.*
8. *Ibid.*
9. *The Joint Lessons Learned Information System (JLLIS) database contains thousands of observations gleaned from a wide variety of exercise and real-world scenarios.*
10. *Joint Staff J-7 defines ‘insight’ as “the act or result of apprehending the inner nature of things,” and a ‘best practice’ as “best actual performance or application [of an insight]”.*
11. *Paraphrased from Joint Operations IO Insights and Best Practices, 3rd Edition (12 Jan 2011), p. 21.*
12. *I&BP, 3rd Edition, Section 3.3, pp. 25-26.*
13. *U.S. Department of Health and Human Services, Administration for Children and Families Program Announcement. Federal Register, Vol. 68, No. 131, July 2003.*
14. *Interestingly, the reference to cross-community application disappears from the description when the word within the healthcare industry, as the inference of cross-community application is implied.*
15. *JLLIS User’s Guide, p. 5*
16. *CJCSI 3150.25D, Enclosure A, p. A-3, Paragraph 2.b.*
17. *CJCSM 3150.25, Joint Lessons Learned Program, 15 February 2011, Enclosure B, p. B-1, Figure 1.*
18. *CJCSI 3150.25D, Enclosure A, p. A-3, Figure A-2.*
19. *CJCSI 3150.25D, Enclosure A, p. A-5, Paragraph 2.c.*
20. *Discussions with Joint Staff J-7 reveal that after a lessons-learned team briefs a combatant commander on its findings and recommendations, follow-on implementation may not occur. J-7 has no leverage to mandate CCMD implementation of a best practice.*
21. *JLLIS is used from the inception of an observation as a tool to manage it through its lifecycle. It’s introduction here is not meant to imply it’s usefulness is limited to Implementation.*



Mr. Bruce Judisch is a senior analyst with MeriTec Services currently working in the Advocacy Branch of the JIOWC’s Advocacy and Force Development Division. Retired from the Air Force, he has over 40 years experience in defense intelligence, programming, and requirements management. He currently supports the J55 Directorate at the Joint IO Warfare Center in San Antonio, Texas.

Global Information Operations Collaboration

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

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

Virtual Collaboration for the IO Community Including Allied Partners



Joint Information Operations Assessment Methodology

By
Mr. Charles Chenoweth

Editor's Note: Assessment of the effectiveness of all military lines of operation is extremely important. Policy makers, senior leaders, and budget makers need good analysis and feedback to justify expenditures. In IO this process is sometimes very difficult. Mr. Chenoweth's essay is a primer for the IO community to find a way to "Assess IO" more effectively.

In this era of declining budgets and shrinking force structures, there is more emphasis than ever on proving the value of a given program. Such proof is hard enough for major weapons systems, but it is an even more daunting task to assess Information Operations (IO) in a way that provides a rapid feedback loop to commanders engaged in operations while also answering the inevitable "so what have you done for me lately?" question from military leaders, Congress, the media, and the American public. While we are unlikely to discover the IO assessment Holy Grail anytime soon, we must redouble our efforts to build a formal, repeatable, user-friendly and value-added IO assessment methodology. We owe it to the warfighter, and we owe it to the taxpayer.

Many aspects of joint operations are quantifiable (e.g., movement rates, fuel consumptions, and weapons effects), and assessing their effectiveness is generally straightforward. However, the dynamic interaction among friendly forces, complex adaptive adversaries, and populations makes assessing less quantifiable operations difficult; for example, assessing the results of measures taken to convince a populace to support their

central government. As planners assess human behavior, they draw on multiple sources across the information environment (IE), including both objective and subjective measures to render a more informed assessment.¹ The goal is to analyze and inform on the performance and effectiveness of executed IO activities for multiple purposes: (1) provide an accurate feedback loop to the commander and his staff; (2) provide opportunities for decision makers to identify information-related capability shortfalls; (3) identify policy and resource issues that impeded joint IO effectiveness; and (4) provide the programmatic community with relevant information to assess return on investment (ROI).

Simultaneous with the recent far-reaching changes across IO, there has been an unremitting demand signal from all quarters for better and more robust IO assessment mechanisms. This was partly a result of Congressional inquiries and DOD scrutiny of IO effectiveness. In his 25 January 2011 memorandum, Secretary of Defense Robert Gates noted, "... combatant commanders have consistently communicated to me the importance of maintaining adequate resources and funding levels to conduct critically important information programs..."² The Joint Staff Deputy Director for Global Operations, Brig Gen Jack Shanahan cited "an overdue focus on regaining efficiencies," or proving the value of the next dollar spent on IO programs, as one of the other drivers for accurate IO assessment.³ With its transfer from USSTRATCOM to the Joint Staff as a Chairman's Controlled Activity (CCA) on 1

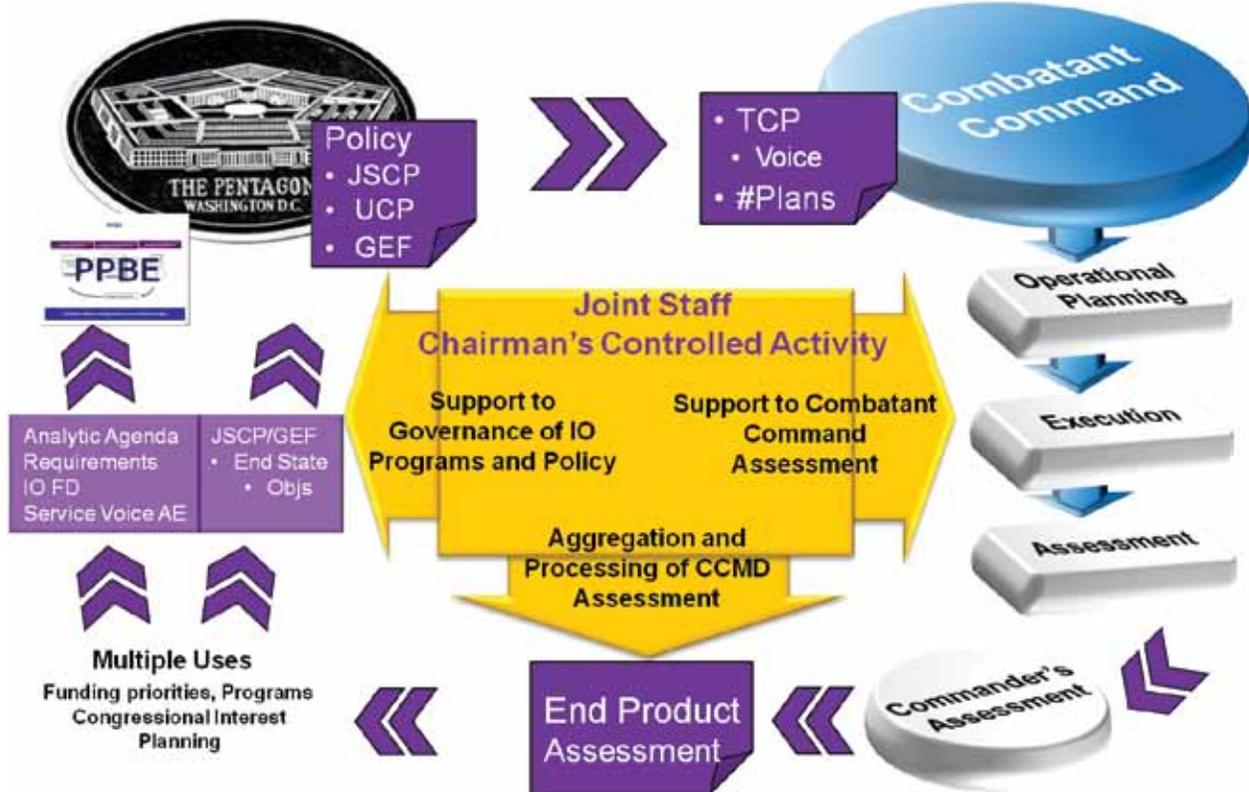


Figure 1. Joint IO Assessment Environment Construct

October 2011, the JIOWC was tasked to develop an IO assessment methodology in support of the combatant commands (CCMD). One of the first and most important lessons learned through initial interaction with other organizations was the overarching imperative to define exactly what is meant by 'IO assessment'.

IO assessment is a continuous process that measures the overall effectiveness of employing joint force capabilities during military operations in the IE. The IE consists of three dimensions: cognitive, physical, and informational. These three dimensions provide the ways to influence the target audience via specific means. The target audience is an individual or group of individuals selected for influence.⁴ 'Means' are the resources available to fulfill the objectives. 'Ways' are how means can be applied to achieve a desired outcome. Activities are conducted in the IE to influence a target. The revised definition of IO, which Secretary Gates highlighted in his January 2011 memo and which will be included in the upcoming revision to Joint Publication 3-13, Information Operations, identifies these activities as "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."⁵ Information-related capabilities (IRC) may be regarded as the tools and techniques utilizing a dimension within the IE that generate an end.⁶ IRCs

include computer network operations, military information support operations, electronic warfare, military deception, operations security and others.

As noted, the demand for better assessment reporting is generated by commanders who need to know if their IO programs are effective or not, and by policy makers trying to determine what resources are needed to effectively execute activities in the IE. In basic terms, the question answered by these assessments is how much money is needed to execute the proposed operation, and is the expected cost worth the expected outcome? The joint IO assessment environment framework depicts the view from the joint force commanders and policy makers.

The construct begins with guidance and policy. Campaign plans link shaping activities to strategic and military end states. For example, the CCMD Voice operations are designed to support end states and objectives stated in the theater campaign plans (TCPs). CCMDs execute the TCPs or numbered plans within their area of responsibility. IO assessment is integrated into both the development and execution of the plans. IO assessment data are analyzed and used by the CCMD planners and executors to evaluate objective attainment. The intelligence community is then tasked to collect information that will be used to make decisions regarding the activities; i.e., adjust activities supporting the plan or discontinue activities.

Assessment data also goes to the commander's strategic assessment staff, which creates the commander's overall assessment of the operation. The commander's assessment is then submitted to the Office of the Secretary of Defense (OSD) and the Joint Staff (JS), who can use it to analyze and modify national objectives. These assessments also go into validating programmatic decisions. IO program executive agents and the JS or OSD resource managers may use the assessments to develop budget and resource plans. Finally, IO assessments can be useful to Congress to help judge its effectiveness on achieving national objectives for ROI analysis.

Among the JIOWC's new essential tasks is to provide combatant commanders with the tools and processes to support IO assessment. No one expects these processes to be completely uniform. Through mission analysis, however, we developed a methodology broad enough to accommodate varied CCMD worldviews while also ensuring normalization across DOD. The joint IO assessment methodology, validated and refined by the IO assessment working group at the 2011 Phoenix Challenge conference, begins with integrating IO assessment into the leading elements of the plan. Though the steps of the IO assessment methodology appear linear, as with almost everything else associated with IO the process is far more iterative and interactive than it first appears. Though the methodology comprises eight steps, this article discusses steps



Guam Congressional Rep. Madeleine Bordallo on an Operational Assessment Tour in Afghanistan

Source: defenseimagery.mil

0 through 3, followed by discussion of analytic models and effects that are hard to measure. The next issue of IO Sphere will cover Steps 4 through 7.

Characterization of the IE (Step 0) initiates assessment and serves as the impetus to initiate planning. It starts and supports development of the assessment baseline. Characterization of the IE is conducted by intelligence personnel, planners, and other staff personnel using a variety of sources such as academia, news media, other government agencies, and industry. As elements of the IE change, the characterization may need periodic refreshing.

In Step 1, integrating IO assessment into plans, planners must develop an executable assessment plan tailored to an IO-related activity or program that notifies all responsible offices of the assessment and its scope. Planning for IO assessment is part of broader planning; that is, IO assessment is not duplicative, it is an essential part of IO planning. Development of a stated IO assessment methodology is intended to make the planner aware of specific steps and sub-steps that make assessment more deliberate in a purposeful way. Integrating IO assessment into plans provides realistic language to assessment activity, supports development of MOPs and MOEs that are measurable, increases awareness of planning staffs of the importance and value of IO assessment,

and provides a vehicle to evaluate resource allocation for IO activities.

Commanders and staffs derive relevant assessment measures (measures of effectiveness [MOE] and performance [MOP]) during the planning process and reevaluate them continuously throughout preparation and execution. They refine these measures in the JFC's planning guidance and in commander and staff estimates, war-game the measures during course of action (COA) development, and include the MOEs and MOPs in the approved plan or order. Planners define and develop indicators for the MOEs and MOPs. During the planning process, (Step 1 of Assessment Methodology) they also develop logic or analytic models of process.

The development of MOPs and task metric development is normally conducted concurrent with or shortly following the COA development phase of the joint operational planning process, while MOEs and indicators for desired and undesired effects come into play immediately after the identification of these effects.

Since the intent of the MOEs and indicators is to build an assessment metric rather than a COA, the development of MOEs and indicators is not dependent upon which key nodes are selected for action. The planning staff returns to the analytic model developed earlier during

planning, (Step 1 of the Assessment Methodology) that best fits with the type of operation to be conducted. Planners then define and develop indicators.

Step 2 involves developing information requirements toward a collection plan. An integrated data collection management plan is critical to the success of the IO assessment methodology and should entail all available tactical, theater and national intelligence sources and other resources. A significant initial intelligence effort to characterize the IE (Step 0) that continues on through the building of an IO baseline (Step 3) helps the commander shape his intent.

Step 3, building an IO assessment baseline provides situational awareness to planners and assessors, better preparing them to develop or modify collection requirements. During assessment integration, the joint IO assessment process will be iterative in nature with intent, objectives, end state, and the collection plan being modified as the baseline evolves and more accurate information is developed. Intelligence community involvement through the entire process from joint intelligence preparation of the operational environment through plan execution is essential. Once joint IO activities are executed, a follow-on dataset is collected, and the change of conditions from the baseline is analyzed to assess the impact of the activities on achieving the desired

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

Figure 2. Joint IO Assessment Methodology

objectives and end-state. This process results in an assessment report with recommendations for plan adjustment, analysis of ROI, and a revised baseline of the desired end-state.

A more refined commander’s intent, objectives, and end state are vital to improving the rigor of any assessment. To assess progress against the objectives, the commander’s intent needs to describe movement from the baseline toward the end state. The example below includes commander’s intent, objectives, and end state.

Commander’s Intent: “I intend to support the Government of Orange and alliance efforts to counter violent extremist organizations (VEOs) by countering their recruitment, financial and propaganda support in the country of Orange. I will emphasize counter-financial activities and counter-propaganda activities while accepting risks in counter-recruitment.”

• Methods:

- Influence and persuade target audiences to support efforts to disrupt VEO activities.
- Counter VEO propaganda (web sites, interactive web, TV, radio, etc...).
- Engage senior regional civilian and military leadership ISO current alliance efforts.
- Discredit VEO financial support mechanisms in the region.
- Share intelligence on VEO activities with regional partners.

• End State:

- Regional stability is enhanced through the degradation of VEO operations.

• Objectives:

- Financial resources are degraded.
- Recruitment capabilities are diminished.
- Propaganda activities are disrupted.

Throughout the planning and assessment process, planners are involved in decision making. “Decision making can be viewed as a conversion process in which the inquiring system

takes inputs (a problem that requires solution) in the form of evidence and information and converts them into outputs (a problem solution or system design) in the form of decisions or solutions.... Modeling is explained as an iterative decision-making process which takes place in the context of a particular inquiring system.”⁷ During the planning process, (Step 1 of the Assessment Methodology) is when general analytic or logic models are used or when models specific to the information environment are developed. Commanders and staff should employ models that fit their mission. Utilizing such a model visualizes for the planners a thought process for development of the activities to achieve the objectives. One objective of models is to attempt a simplification of the real-world situation through abstraction. During planning, using an existing model or developing a new model that displays the same characteristic or properties as the slice of the world from which it has been extracted helps planners visualize the problem at hand.

Assessment Analytic Models

A useful example of a general analytic model is the Hierarchy of Evaluation. This model can visualize for the assessment staff assessment principles as they relate to the military planning process. Level 1 of the model in military planning would be part of characterization of the environment (Step 0 of the Assessment Methodology) and is the foundation where evaluation focuses on the problem to be solved or goal to be met, the population to be served, and the kinds of services that might contribute to a solution. Level 2 could be characterized as mission analysis, (Step 1 of the Assessment Methodology) and addresses the design of a policy or program and seeks to confirm that what was planned is adequate to achieve the desired objectives. Level 3 is similar to COA development, but could also include development of a collection plan and a baseline, (Step 1, 2 and 3 of the Assessment Methodology) and asks whether execution met the design at Level 2. Level 4 includes MOE and MOP development and also addresses the assessment data analysis, (Step 1 and 6 of the Assessment Methodology) where outputs are the products of program activities and outcomes that are the changes that result. Level 4 is the first glimpse of potential

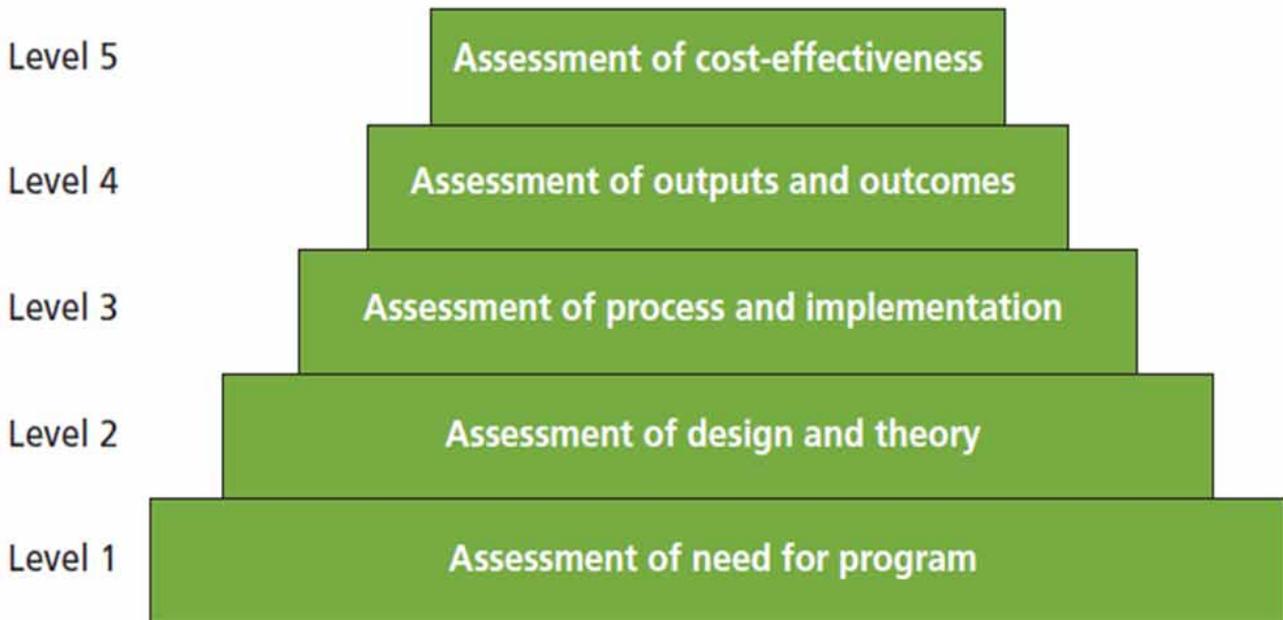


Figure 3. Hierarchy of Evaluation

solutions. Finally, at Level 5, the assessment looks across programs for cost-effectiveness or “bang for the buck.”⁸ This relates to Step 6 of the Assessment Methodology.

A second example of a logic model is used by military information support operations (MISO) assessment staff. This model has been used for decades as a tool for evaluating programs in a variety of settings. It is a graphic depiction of a process that communicates the underlying assumptions upon which an activity is expected to achieve a particular result. When used as a tool for planning and evaluating programs, the model is useful for predicting and articulating program outcomes. If used correctly, it will provide most, if not all, of the necessary information to describe a program’s explicit goals, underlying assumptions and means of gauging a program’s effectiveness. The Inputs and Outputs columns relate to Mission analysis and course of action development which is in Step 1 of the Assessment Methodology. The Outcomes columns relate to MOE development also part of Step 1 of the Assessment Methodology. Thus, within the context of MISO, the model becomes a tool for organizing and communicating information that is already integral to the MISO planning process.

Here we get to the critical issues in IO assessment. How do you develop good indicators? How do you measure things

that are difficult to measure? We collected a few best practices during our initial analysis, and the JIOWC will continue to focus on consolidating and categorizing them. They include looking for inverse indicators, or the absence of something. On difficult measurements, the robustness of MOP may be an indicator of MOE. For example, the number of persons reached may indicate that the MOE is trending positively. Also, an individual’s response (small sample) may provide an indicator. Another tactic may be to develop a robust definition of what you expect to see should an MOE track positively.

A particularly difficult assessment problem may have more ethereal indicators that force us out of the normal planning process. One proposed way is to build the model by analyzing commander’s intent during the mission analysis phase; that is, answer the question, “Why are the objectives important in the context of the associated desired end states?”, then collect the answers in concise narrative form. The narrative generates metrics— i.e., things we want more of and things we want less of—and bins these into topics of interest. The narrative is the summary of subject-matter experts’ opinions on how the environment works, (this provides context and clarity for planners, executors and collectors) within the context of the objectives, end states, ways, and means. The logic within the narrative provides a qualitative understanding of what is

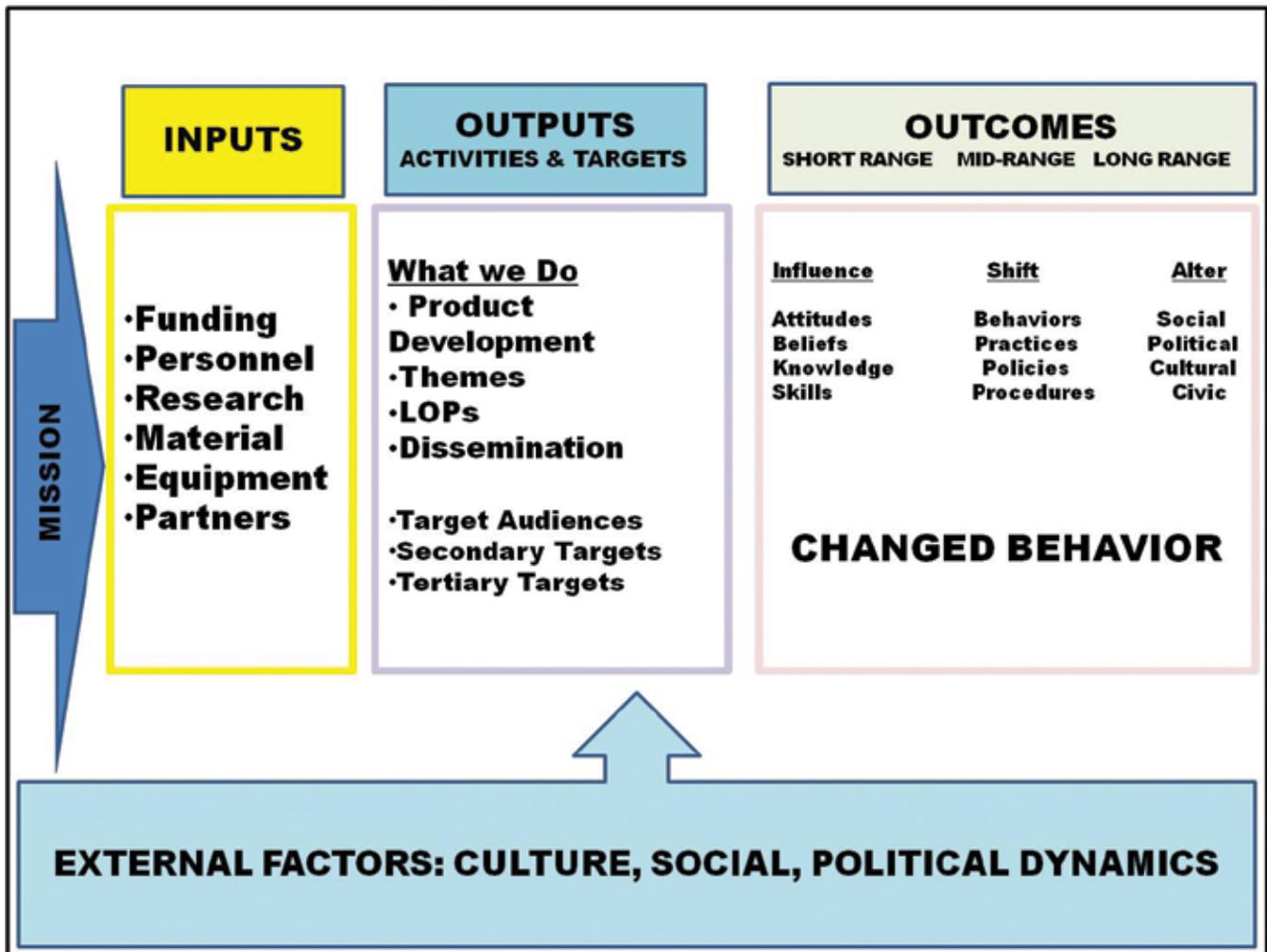


Figure 4. Military Information Support Operations (MISO) Model

likely to happen as IRC activities alter the qualitative and quantitative values of the metrics.

The assessment team then uses professional subjective judgment and the logic within the narratives to assess the implications of the collected metric information against the postulated assessment question. Write the assessment question; for example, "What is the likelihood of, and what are the risks to, the conditions for the specified end states occurring or remaining stable if the region transitions from coalition force control to national government control?"⁹ Then provide the question to the collectors and allow them to evaluate the conditions rather than just have them count individual indicators.

This is just a start. I hope we whet your appetite for more. In the next edition I will provide more information on Steps 4 through 7 of our proposed joint IO

assessment methodology. If you have a better idea, or would like to support our ongoing assessment initiative, contact the JIOWC. There is no better time to improve IO assessment—you can be part of the solution. ●

Endnotes:

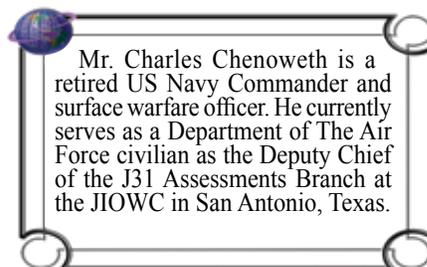
1. *Joint Publication 5-0, Joint Operations Planning, 11 August 2011.*
2. *Secretary Robert Gates, Strategic Communication and Information Operations in the DoD, 25 January 2011, SECDEF Memo.*
3. *Brig. Gen. John N.T. Shanahan, Information Operations in an Age of Shrinking Budgets: Crisis or Opportunity, IO Sphere December 2011 Joint Publication 1-02, DOD Dictionary*
4. *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms, amended through 15 September 2011.*
5. *SecDef Memo, 25 Jan 11, Strategic Communication and Information Operations within DoD.*

6. *Proposed definition for JP 1-02.*

7. *John P. van Gigh, System Design Modeling And Metamodeling, Plenum Press, New York, 1991.*

8. *Richard A. Berk and Peter H. Rossi, Thinking About Program Evaluation, Newbury Park Calif.: Sage Publication, 1990.*

9. *Stephen Downs-Martin, Operations Assessment in Afghanistan is Broken. What Is to Be Done?, Navy War College Review, 2011.*



MAKE A DIFFERENCE JOIN THE FA 30 TEAM



Become a US Army IO Officer



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

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

CHECK OUT THE IPO WEBSITE

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

Assessing COIN Information Operations Aimed at the Local Population

By

Stephen Downes-Martin, Ph.D.

Editor's Note: Dr. Stephen Downes-Martin is one of the foremost authorities on operational assessment in DOD. He approaches the assessment question and problem from a commander's objective and decision-making framework using logic. Some of his views may be considered controversial, but they are worth study and discussion as we find a way to "Assess IO."

If we are to take the population-centric view of counter-insurgency (COIN) seriously, then the perceptions of the population about the Government's legitimacy or the capability and capacity to provide security, governance and economic opportunity, or those of the insurgents, must be a key objective of information operations (IO).¹ It is based on perceptions such as these that individuals and the population at large make the decision to support the Government and its security forces or the insurgents. Therefore, a critical effort of IO in support of COIN must be aimed at influencing these perceptions of the population and of the population's thought leaders towards supporting the Government and its security forces and opposing the insurgents. The same is true for the insurgents, who will be working to influence the population's perceptions and decisions to support them and oppose the Government. The population-centric view of COIN requires a perception war using IO between the Government and the

insurgents over the perceptions and decisions of the population. Core to assessing progress in the application of IO in perception warfare is the requirement to forecast the future decisions of a population and individual thought leaders resulting from an IO. Modern research in psychology and decision sciences identifies two fundamental problems that must be addressed: people cannot actually predict their own, let alone other people's, decisions under different information circumstances, and; experienced people become over-confident in their abilities to control situations when those situations are novel. Unless explicitly dealt with, these problems lead IO planners and assessors into believing they are being effective when they are not. This paper describes these problems and suggests methods for circumventing them.²

The IO Assessment Question

There is a problem with the 25 Jan 2011 SecDef Memo on "Strategic Communication and Information Operations within DoD"³ in that it defines the purpose of IO as "*to influence, disrupt, corrupt, or usurp the decision-making of adversaries.*" This definition ignores IO aimed at the population and their thought leaders whose decisions ultimately decide the outcome and the success or otherwise of the COIN campaign. Unless one is going to ignore the perceptions of the population being contested by the insurgents (or, worse, treat them as an adversary), then clearly the population-centric view of COIN requires us to expand the IO definition from "adversaries" to "stakeholders" (which includes the insurgents, populations, allies, media, etc.). We must take care to disentangle two very different targets of IO. First, with respect to targeting insurgents the purpose of IO becomes "*to disrupt, corrupt or usurp the decision making of the insurgents in order to influence the insurgents to make decisions that are advantageous to us or disadvantageous to them, or to influence the insurgents to fail to make decisions that are disadvantageous to us or advantageous to them.*" Second, with respect to targeting the population and their thought leaders, the purpose of IO becomes "*to influence the perceptions of the population and their thought leaders to encourage them to make the decision to support the Government and their security forces and to oppose the insurgency.*"

Whichever the target, one must assess the progress of the IO and we may use doctrine for guidance. The purpose of operations assessment is to support the commander's operational or strategic level decision making. Joint doctrine describes assessment as "*a process that measures progress of the joint force toward mission accomplishment.*"⁴ Joint doctrine also makes clear that simply measuring progress is insufficient, that the assessment process must "*help commanders adjust operations and resources as required, determine when to execute branches and sequels, and make other critical decisions to ensure current and future operations remain aligned with the mission and military end state.*" (JP 3-0, p. IV-31) Operational and strategic decision-making deals with future problems, not current tactical battlefield problems. Therefore, by definition, operations assessment must attempt to forecast future obstacles to achieving operational or strategic objectives in time for



Combat Camera Documenting Damage in Mostar Bosnia-Herzegovina During Operation Joint Endeavor in 1997
Source: defenseimagery.mil

the commander to plan around those obstacles. The most problematic obstacles will be those deliberately generated by the opposing forces. So, in order to provide decision support to the commander within the guidelines laid down by joint doctrine, operations assessment must answer what I call “the assessment question”²⁵, which for IO has the general form: *“What is the likelihood of the insurgent or the population making the decisions we want, or not making the decisions we do not want (by the specified future date/time), what are the obstacles to influencing those decisions, what is the likelihood of failing to influence those decisions in the ways that we want?”*²⁶

Attempting to influence perceptions of, and forecast future decision making by, individuals and groups during COIN and irregular warfare (IW) is highly problematic due to the increasing emphasis of political, economic, social, infrastructure and ideological factors compared to kinetic military considerations, made worse by the ubiquitous presence of media. Nevertheless, influencing the perceptions of others and forecasting their decisions is what one must do to implement and assess an effective IO in modern conflict.

Military Expertise is Not Enough

Traditional tactical attrition warfare is relatively simple to assess. The possible and likely future outcomes of interacting protagonist decisions are driven by physics (for example external ballistics, logistic flows, time and space factors etc.) and the statistics of millennia of small unit actions. We know these physics and statistics rules, and so assessors use these to identify the range of what could happen and what is likely to happen in the future resulting from interacting protagonist decisions. They take into account cultural and morale effects using civilian advisors.

Many of the modern conflicts in which we are interested do not have an associated physics, case studies or statistics on which to base assessment. For example, what are the rules (the equivalent “physics” and “statistics”) for identifying possible outcomes of an IO during a COIN in which one or more of the regional powers have nuclear weapons? How many of these have occurred? I suggest near zero is a reasonable answer for most of the problems in which we are interested. Modern operational and strategic level COIN and IW are driven by complex interacting political, military, economic, social and ideological effects, most of which we do not understand or at most have only an intuitive grasp, and for which we do not have a statistically valid sample set of previous situations on which to draw.

A common approach to assessment is to use advisors, often civilians, who are subject-matter experts in the appropriate non-military areas. The assessors draw on their advice to identify the range of possible outcomes to interacting protagonist decisions. Then, drawing on their military experience, they decide which of these outcomes are likely to occur and whether they constitute obstacles to success. The assessors and their advisors have to attempt to forecast decision makers from other cultures. Mirror imaging is a problem when we are interested in friendly decisions in the face of hostile intentions, or are interested in hostile decision-making behaviors. Obtaining experts in hostile thinking generates several problems. Ex-patriots from hostile countries or cultures of interest often have various political agendas, are not necessarily expert in their own country’s or culture’s political and military decision-making styles (how many disgruntled Americans are truly expert on the political and military culture of the US?); and they face security classification issues. US citizens who are genuinely expert in foreign cultures

and who can obtain security clearance are rare, and we can only assume that their interpretations of foreign cultures’ decision-making are accurate.

Assessors Can’t Predict Decisions

Information operations attempt to influence the decision making of individual thought leaders of a population and of key groups within the population. However, research shows that “People are not aware of the reasons that move them; even an introspective person with incentives to estimate how he or she would have behaved with different information cannot do this.”²⁷ However, this is precisely what we ask IO planners, operators and assessors to do: to imagine that they or their target is in some future (or other) environment, which is different from the present one due to an IO and predict the decisions they or their target would make due to that operation. Since most people cannot accurately predict their own decisions, then they certainly do not make good predictors about other peoples’ decisions, i.e. the population’s thought leaders or groups within the population. These problems are exacerbated when the decision makers are from a different culture.

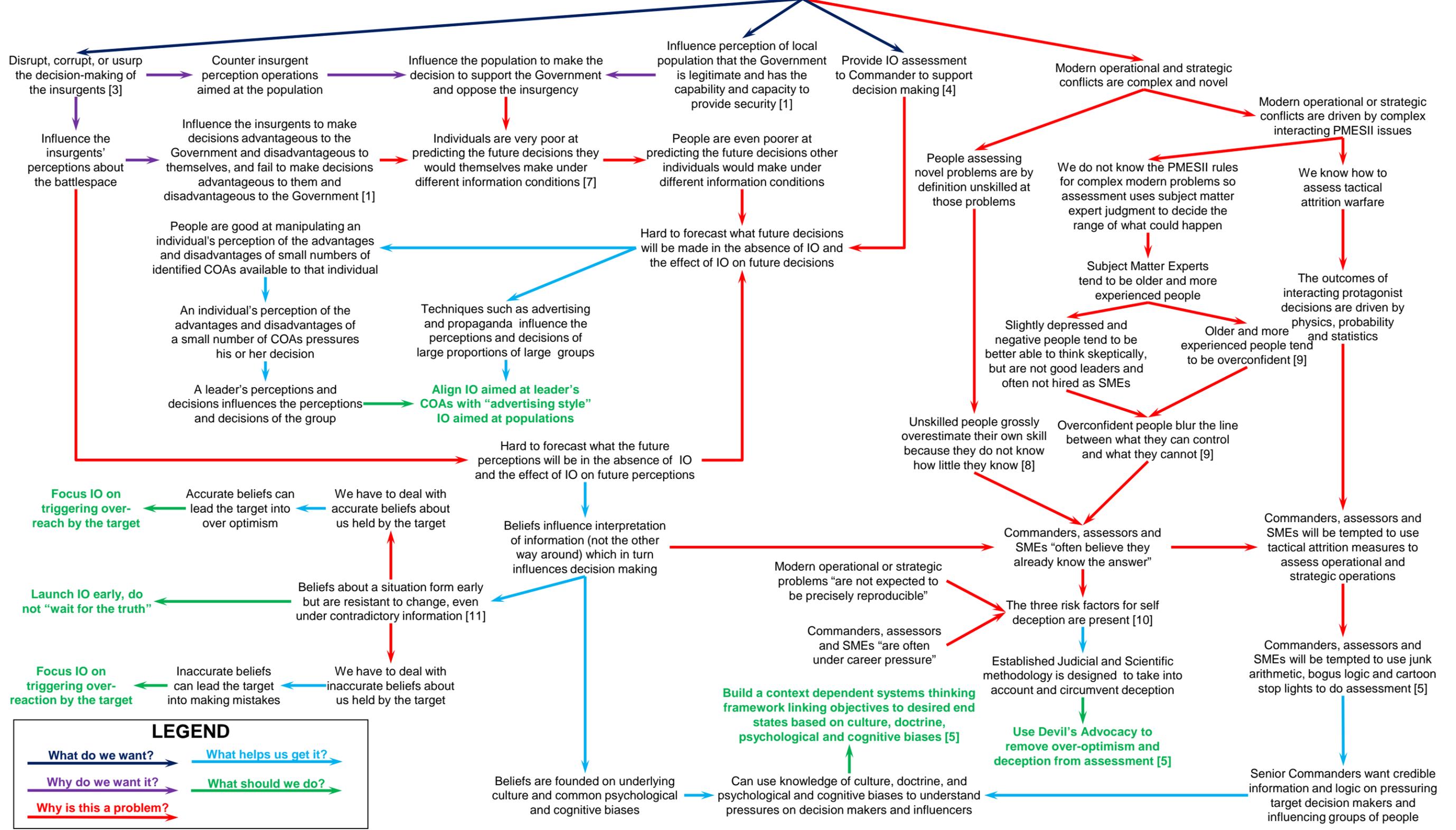
Although the advertising industry has great success in predicting and manipulating the decisions of percentages of large populations, it cannot credibly predict the decisions of pre-specified individuals or pre-specified small groups. What one can do is identify the courses of action (COA) probably available to key target decision makers, and then apply pressures to attempt to influence the perceptions of the advantages and disadvantages of these COAs in the mind of the target. This does not allow us to predict the decision a specified decision maker will make, since we know that different people faced with the identical advantages and disadvantages to the same alternative COAs can and do select different COAs based on their choices of which disadvantages to suffer in order to gain which advantages. The more one knows about the individual decision maker, the more likely one can construct an information environment that increases the advantages and decreases the disadvantages in the mind of the target of the decision we want relative to the other COAs. After the target makes a decision, it is extremely difficult to prove he would not have made it absent our IO (even asking the target does not work, since individuals are very poor at predicting what they themselves would decide under different information environments). In addition, we do not and cannot know at what point the target will tip from a decision we do not want to a decision we do want.

The two very different types of operation must be aligned: manipulating the perceptions of the advantages and disadvantages of COAs in the minds of key target individuals (whether thought leaders of the civil population or commanders of the insurgency), and; shifting the perceptions of large specific groups within a population (or within the ranks of the insurgency). Assessing IO focuses on how well we are applying pressure to the advantages and disadvantages in the mind of target individuals and how well we are pressuring local cultural norms concerning the conflict. To do this we need to identify a range of possible future decisions (in response to the pressures) along with an indication as to whether the pressures are increasing or decreasing.

Assessors are Over-Confident

If the conflict environment is novel—as is the case for IO in modern COIN and IW—then assessors and their subject-matter-expert advisors are by definition unskilled at assessing operations within the conflict precisely because they are

Population-centric Information Operations in Counter Insurgency



novel. They have no statistics and only analytical case studies to draw on, and little proven experience. Three effects demonstrated by psychology research and fraud analysis work together to make this a serious problem for assessment.

First, research shows that people in the lowest quartile of actual competency tend to assess themselves in the second to highest quartile; i.e., their incompetence robs them of the ability to realize they are incompetent. People in the highest quartile of actual competency tend to assess themselves slightly lower but within the highest quartile; that is, they inflate their colleagues' competency compared to their own.⁸ Put crudely, unskilled people are unaware of it.

Second, research shows that older and more experienced people tend to be overconfident in their ability to control events that are in fact outside their own control while failing to realize the need for adapting their thinking.⁹ Their success in the past leads to confidence, which in competitive situations can mask their lack of competency through successful bluffing. Their successful control of past situations leads them into the mistake of believing their competency applies to current situations involving chance.

Third, three risk factors have been identified in nearly all cases of scientific fraud: the perpetrators "were under career pressure"; they knew, or thought they knew, what the answer to the problem they were considering would turn out to be if they went to all the trouble of doing the work properly; they were working in a field where individual experiments are not expected to be precisely reproducible."¹⁰

In modern complex conflicts, these effects are likely present for experienced senior people. Their future careers clearly depend on their success in the operation. Older and more experienced people tend to be unaware of their lack of skills in novel situations and tend to be overconfident, and modern complex conflicts are unlikely to be precisely reproducible. The presence of these three risk factors imply that self-deception by assessors must be considered to be likely present amongst senior military assessors and any civilian advisors.

What is to be Done?

First, note a set of four observations: "we tend to perceive what we expect to perceive; mind-sets tend to be quick to form but resistant to change; new information is assimilated to existing

images; initial exposure to blurred or ambiguous stimuli interferes with accurate perception even after more and better information becomes available."¹¹ In summary, beliefs are remarkably robust, even under contradictory evidence. Therefore, an IO should avoid falling into the trap of trying to change a target's mind-set to trigger a desired forecasted decision. An IO should focus instead on strengthening already held beliefs to trigger overreach by the target when we know the target's beliefs are inaccurate, and overreaction by the target when we know the target's beliefs are accurate. The latter is especially useful if the target has accurate beliefs that are shameful to the Government and its security forces. One way of systematically thinking about a target's belief structure is to develop a systems-thinking model of the target's information environment and the target culture's likely reaction to different information.¹²

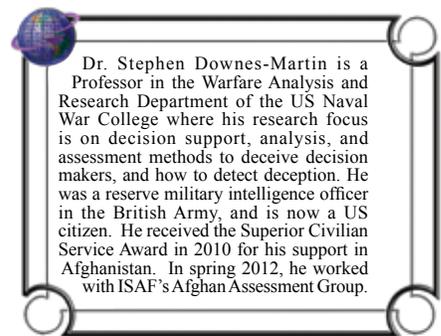
Second, IO assessors must consciously avoid the trap of being overconfident in their ability to influence and forecast target perceptions and decisions. One way to do this is to use devil's advocacy, in which one argues the optimistic case both for and the pessimistic case against a forecast of a desired outcome (similar to the testing of evidence by the prosecution and defense in a law court), and then makes a final judgment based on the two cases. If the resources are available, have separate teams do the optimistic and pessimistic assessments and argue their respective cases to a senior assessor for final assessment. Otherwise, do the pessimistic assessment first. Be rigorous and ruthless when doing the pessimistic assessment; any squeamishness here will result in challenges to the final assessment in what could be an embarrassing public arena. When judging between the optimistic and pessimistic assessment, pay particular attention to pessimistic items that overwhelm positive ones and to positive items that fix negative ones.

Endnotes:

1. US Army Dept., "Counterinsurgency," *Field Manual 3-24* (Washington, DC, 15 December 2006). (FM 3-24 is also issued by Headquarters, US Marine Corps, as *Marine Corps Warfare Publication [MCWP] 3-33.5*)
2. I will use the term *Information Operations (IO)* throughout this paper to avoid the sterile debate concerning the use of terms like *Psychological Operations* and *Military Information Support Operations (MISO)*. These latter are a subset of IO, and so anything true about them is by definition

true about IO (but not vice-versa). The types of IO discussed in this paper are clearly psychological in nature; however, I do not discuss the physical means by which they are implemented.

3. SECDEF Memo 25 Jan 11 "Strategic Communication and Information Operations within DoD."
4. US Joint Staff, "Joint Operations," *Joint Publication 3-0* (17 September 2006, incorporating change 2, 22 March 2010), p. IV-30; US Joint Staff, "Joint Operation Planning," *JP 5-0* (26 December 2006), p. III-57.
5. Stephen Downes-Martin, "Operations Assessment in Afghanistan is Broken: What is to be Done?" *Naval War College Review*, Autumn 2011, Vol. 64, No. 4, pp 103-125.
6. Note that the adversary not making a decision he would otherwise have made is in fact a decision.
7. Robert Jervis, "Reports, Politics, and Intelligence Failures: The Case of Iraq," *Journal of Strategic Studies*, Vol. 29, No. 1, 3 – 52, February 2006. See also Robert Jervis, "Understanding Beliefs," *Political Psychology*, vol. 27, Fall 2006.
8. Kruger J, Dunning, D., "Unskilled and unaware of it: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments," *Journal of Personality and Social Psychology*, 1999, Vol. 77, No. 6, 121-1134. See also Timothy Wilson, "Strangers to Ourselves: Discovering the Adaptive Unconscious," *Harvard University Press* 2002.
9. Malcolm Gladwell, "Cocksure: Banks, battles, and the psychology of overconfidence," *The New Yorker* July 27, 2009.
10. David Goodstein, "On Fact and Fraud: Cautionary Tales from the Front Lines of Science," *Princeton University Press*, 2010. See also Michael Shermer, "When Scientists Sin: Fraud, deception and lies in research reveal how science is (mostly) self-correcting," *Scientific American*, July 2010.
11. "Psychology of Intelligence Analysis," Richards Heuer, *CIA* 1999.
12. See reference 4 for a description of one way to build such a systems-thinking model.



JOINT ELECTRONIC WARFARE THEATER OPERATIONS COURSE



SAN ANTONIO, TEXAS

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

Information Environment Training and Education Considerations for the Joint Force 2020

By

Colonel Carmine Cicalese, US Army

Editor’s Note: Colonel Cicalese is a staunch advocate of professional military education for IO warriors. His participation and vision in the future of the IO force is a critical contribution to force development and professionalizing IO planners and specialists in the joint and service forces.

Even as the Department of Defense (DOD) heads toward a leaner fiscal future, senior leaders are emphasizing the importance of dedicating more resources toward training and educating. Chairman Dempsey, when serving as US Army Training and Doctrine Commander, remarked, “To preserve this great legacy, it is our obligation to ‘keep first things first’ and ensure leader development remains our first and foremost priority.”¹

To highlight a renewal of Joint Professional Military Education (JPME), the Chairman continued the Joint Staff reorganization his predecessor started and elevated the Joint Staff J-7 position to a three-star position. General Dempsey also issued the Chairman’s Strategic Direction for 2020, which details the need to prepare the force through an intense focus on training and education. This includes the key tasks to “Define the essential knowledge, skills, attributes, and behaviors that define the Joint Profession of Arms” and to “Institutionalize these in education, training, organizations, and policies.”²

General Dempsey recognizes that training and education go hand-in-hand. He affirmed this in his recent memorandum to the President of National Defense University, articulating the new NDU mission to provide rigorous JPME and to center the main effort on providing JPME on the conduct of joint training,

research and outreach.³

Meanwhile, several military information-related capabilities (IRC) and processes that impact the information environment (IE) are growing. The Services have established Cyberspace Component Commands to complement United States Cyber Command.⁴ The United States Army Special Operations Command established the Military Information Support Command and has added another group-level command.⁵ The United States Air Force continues to increase the number of Behavioral Influence Analysts, integrating these personnel into joint commands.⁶ More conferences and professional discussions are focusing on the convergence or overlap of these processes and mission areas.⁷

While individual IRCs have grown in size and importance over the last ten years of conflict, those days are coming to an end. As Brigadier General Shanahan, Joint Staff J-39 Deputy Director of Global Operations (DDGO), noted, “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.”⁸ Simultaneously, improving military operations in the IE across the board is uniformly recognized as a critical requirement.⁹ Despite the growing fiscal constraints within DOD, operations within the IE have significant growth potential. To address these crucial issues, this article will discuss the Joint Command, Control and Information Operations School’s (JC2IOS), essential role within the DOD training and education enterprise and recommendations for a way forward.



Allied Exchange Officer Leads his IO Planning Group at the Joint Forces Staff College

Source: Author

The Role of the Joint Command, Control and Information Operations School

To support these trends, the JC2IOS located at the Joint Forces Staff College (JFSC) in Norfolk, Virginia, is posturing itself to be a leader in joint training and education for integrating operations within the IE. The JC2IOS is one of four schools at the JFSC, which is part of the National Defense University enterprise.

The JC2IOS mission is to train and educate national security professionals in applying concepts, capabilities, and procedures associated with planning and coordinating joint, multinational and interagency operations in the IE.¹⁰ This mission complements the JFSC mission, which is to educate national security professionals in planning and executing operational-level joint, multinational and interagency operations. The mission captures two primary, yet distinctly different courses: the Joint Information Operations Planners Course (JIOPC) and the Joint Command, Control, Communications, Computers and Intelligence Staff Operations Course (JC4ISOC).

The JIOPC is a four-week course taught at the compartmented level. It has two derivative courses: the two-week Joint Information Operations Course (JIOC) for allies with collateral access, and the one-week Joint Information Operations Orientation Course (JIOOC) for those with compartmented access needing an IO overview. Students who successfully complete the JIOC and JIOOC may certify the first week of the JIOPC if

they return to complete the JIOPC within one year.

The JC4ISOC is taught in two versions: a three-week compartmented-level class that includes a student trip to the National Capital Region, and a two-and-a-half-week collateral -level class that omits the trip. Both courses culminate in a detailed planning exercise centered on a Humanitarian Relief operation.

In addition, the school educates joint students at the ten-week Joint Combined Warfighting School (JCWS) and the eleven-month Joint Advanced Warfighting School (JAWS). JC2IOS educates over one thousand JCWS students per year via Fundamentals of Unified Action building-block lessons on strategic communication, IO, and cyberspace operations. This lesson has increased from two to three hours, while JAWS students receive over ten hours of instruction on these three topics. JCWS and JAWS students can also choose an eight-hour IO and cyberspace elective. While educating JCWS and JAWS students is beyond the JC2IOS charter and challenges resources dedicated to other courses, the JC2IOS leadership and faculty believe this is the best use of a valuable DOD resource: a competent joint faculty. Understanding the background of these developments is important.

One Man's Vision Guides the School's Future

In 2009, several military IE-related capabilities and processes, like IO and cyberspace operations, competed in a

'flurry of activity' for doctrine, resources and primacy within DOD.¹¹ As the competition came to an apex, the concern over what perspective would prevail precipitated then JC2IOS Director, CAPT (USN) Curtis Phillips to ask, "Who will be looking out for the information environment?" This insightful question stimulated the current JC2IOS leadership and faculty to such an extent that, during the preparation for last year's IO Force Development Summit, the Director and faculty developed the following vision: *JC2IOS is the premier joint organization for training and educating national security professionals who plan or integrate operations in the information environment.*

Even though JC2IOS does indeed train and educate joint students at JFSC, this vision is less than perfect. Within the school, JC2IOS tilts toward training for the known vice educating for the unknown.¹² The JIOPC trains students on one specific task: plan for IRC integration to affect decision making. Yet, each plan is unique, requiring the faculty to educate students on joint planning and Service capabilities in applying the known planning systems and processes against the unknown abstract problems of operational design.

More importantly, JC2IOS recognizes the excellence in IO and C4I education provided by other institutions; e.g., the Naval Postgraduate School (NPS) and the National Defense University. Training is no different; for example, the Joint Electronic Warfare Theater Operations Course in San Antonio, and the Joint Network Attack Course in Pensacola, the



Students Conduct a Planning Exercise as Part of the IO Course of Study at the Joint Forces Staff College

Source: Author

premier joint training venues for electronic warfare (EW) and computer network attack.

Still, the JC2IOS Director and faculty believe in a healthy competitiveness with others to be a premier joint organization for training and education, but with the JC2IOS focusing on the process of integrating capabilities like those in IO, C4I and cyberspace operations at the operational level. Despite its imperfections, the JC2IOS vision has served the organization well toward improving the school's position and product, while enhancing the joint student's experience.

Inside-Out

Within JC2IOS, the faculty—the school's center of gravity—works diligently to improve both JIOPC and JC4ISOC. Lieutenant Colonel Tim Pike led the review and staffing of the JIOPC to open it to other partner nations sharing compartmented access. This February, JIOPC graduated its first foreign officer: Commander Martin Bravery, Royal Navy. Colonel Pike and his experienced faculty recertified the JIOPC and JIOOC as joint courses so graduates can earn points in the Joint Officer Qualification System. In the coming months, JC2IOS should complete joint certification of JIOC.

Concurrently, Commander James Joyner and his top-rated C4I faculty work fervently toward revising the JC4ISOC into a Classroom 236 model paralleling the US Central Command model for Task Force 236. Classroom 236 educates and trains a diverse student body to prepare the commander in management and decision-making. Over the course of two classes, the JC4ISOC witnessed an increase in Joint Operations Center students to complement the bevy of US Navy information professionals who rely on the course as an integral part of their training and education.

The JC2IOS faculty has also improved support to JCWS and JAWS. The SC and IO lessons now include the emerging doctrine for a commander's communication strategy and better employ the Harvard Business School Case Study Methodology.

Lieutenant Colonel Mark Lipin, a USAF cyberspace operator, morphed the C4I elective into the eight-hour Challenges in Cyberspace elective. Colonel Lipin will likely lead an expansion of this elective into sixteen hours. While doctrinally defining cyberspace operations remains elusive, JC2IOS is educating joint students via the JCWS/JAWS cyberspace lesson and electives how to include planning in conducting and executing cyberspace operations within operational design.

JC2IOS continues to deploy mobile training teams (MTT) to the combatant commands. In 2011, the C4I Division employed a one-week MTT-led course for Joint Communications Support Element, USCENTCOM, and USSOCOM students, while the IO Division employed MTTs for two-week courses in Miami, Tampa and Stuttgart for the resident geographic combatant commands (GCC). This training has proven to be value added to the GCCs, as JC2IOS can train and educate more personnel on integrating IRCs at the student's home station, while the GCCs realize a substantial cost savings. Because JC2IOS in-residence and MTT training is the same, students needing certification can split their training between MTT and in-residence training, while others whom don't need the full JIOPC can still receive IO training at their home station. For JIOPC 12-2, three of twenty-one AFRICOM and EUCOM IO MTT-trained students traveled to Norfolk to complete the final two weeks of JIOPC.

Outside-In

As other organizations learned of the JC2IOS vision, they have contacted JC2IOS to assist them in developing curriculum and hosting future courses at the JFSC. Commander Ben Snell and Major Kim Rossiter are applying their expertise in intelligence operations and staffing to assist the Undersecretary of Defense for Intelligence in developing and hosting the Information Environment Advanced Analyst (IEAA) pilot course in August 2012. Most notably, the IEAA leadership recognized Major Rossiter for his distinguished contributions towards enhancing the IEAA curriculum development.



Joint Forces Staff College C4I Students and Faculty Prepare for a Briefing
Source: Author

At the request of the Joint Staff J-39, the JIOPC faculty will travel to Maxwell Air Force Base this April to lead the Senior Joint IO Applications Course general-/flag-officer students with a case-study style planning exercise in joint IO. The Joint Staff has also requested JC2IOS develop a one-week MTT-based IO Overview course designed to educate partner nations on joint and operational level IO. The JC2IOS goal is to develop an unclassified course designed for an expeditious foreign disclosure release review by the beginning of fiscal year (FY) 2013.

Also coming in FY 13, JC2IOS will host two iterations of the Norfolk-based Joint Military-Deception Trainers Course (JMTC). The JMTC and JIOPC leaders are synchronizing the courses such that JMTC students can attend the courses sequentially to maximize their experience in the Hampton Roads area. JC2IOS is also in discussion with Joint Staff J-39 for the Joint IO Warfighting Center (JIOWC) to host the JIOOC in training more personnel on the basics of joint IO, and to save JIOWC personnel an additional week of travel to the JIOPC. Economizing student time—the other most important DOD commodity—is an imperative for tomorrow’s joint training and education institutions.

JC2IOS leadership and faculty continue to engage other IO training and education venues, such as the NPS and the Army Combined Arms Center FA-30 Course, to share curricula. The JC2IOS faculty relishes the annual opportunity to assist NPS students during their planning

exercise. The organizations continue to collaborate toward the goal of Joint Staff validation of the NPS IO track and Army FA-30 Course as JIOPC equivalents.

Future Endeavors

As several military-oriented professional organizations, such as the Association of Old Crows, have noticed, operations in the IE often converge. In previous professional papers, JC2IOS has noted the mission of maintaining the DOD Global Information Grid as part of cyberspace operations has seemingly eclipsed the need to plan for the installation, operation and maintenance of C4I systems. The electromagnetic spectrum is so interconnected with cyberspace that the lines between EW and cyberspace operations seem to blur. Holistic cyberspace operations should include its own IO, while simultaneously supporting a GCC’s IO. Simultaneously, an EW attack that affects cyberspace may support the same GCC IO.

DOD will not be able to cut corners by merging C4I, EW, cyberspace and IRC integration into one or two specialty skills. The days of ‘one and done’ training are over.¹³ Like the Navy’s Information Dominance Corps model, each specialty will need to branch into a broader domain operation, such as cyberspace operations, or a process like IO, as the service member’s career progresses. To echo the DDGO, “we also need everyone to become reasonably proficient in integrating kinetic and non-kinetic, and lethal and non-lethal IRCs (Information Related Capabilities).”¹⁴ Whether it is

integrating IRCs for IO or integrating C4I systems for cyberspace operations, the JC2IOS needs to follow its vision to focus on *joint students who plan or integrate operations in the information environment*.

IO should remain a core competency for JC2IOS. C4I systems-integrations planning should also be taught, but could conceivably become part of a broader Joint Cyberspace Operations Planner Course. JC2IOS can adapt and continue to thrive by supporting individual IRC training, like the JMTC, as well as the broad-based IEAA course. However, courses like the Joint Electronic Warfare Theater Operations Course should remain where the professional expertise exists. Nevertheless, another question remains: How does DOD optimize training and educating the joint force on complex domain operations or processes like cyberspace operations and IO, given the demand on the joint student’s time and the impending personnel crunch on available quality faculty? Leveraging e-learning modalities, such as blended learning, can be one of the key answers.

Blended Learning

Blended learning, the combined use of distance learning and in-residence learning, is the hottest trend in training and education in both military and civilian environments. Blended learning inherently recognizes that students learn and retain information differently, thereby accommodating various learning styles. It also facilitates the potential for cross-service training. If developed smartly and collaboratively, multiple

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.gov/sites/jiowc/home.aspx>

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

**A GLOBAL IO COMMUNITY RESOURCE
ADVOCACY FOR IO**



equivalent non-resident courses could feed a single resident course.¹⁵

To develop this model, JC2IOS will access the Joint Continuing Distance Education School at JFSC, which already graduates hundreds of Reserve and National Guard officers through the forty-week non-resident/resident Adjunct Joint Professional Military Education program. JC2IOS is also coordinating with the Joint Staff J-7 to develop an online course to educate the joint student on the basics of IO. Such an online course could also serve as the future JCWS distance-learning aspect of the IO fundamentals lesson, or perhaps a prerequisite for the JCWS IO elective, or even the JIOPC.

Joint students focusing on operations in the IE face the same dilemma of disparate learning modes and time constraints. For example, a joint officer who attends JCWS may also need to attend the JIOPC or JMTC. JC2IOS and other joint learning institutions need to be looking now at how a joint student of operations in the IE receives the necessary training and education via blended learning. To wit, the US Army information proponent is already designing a blended-learning model to have the Tactical Inform and Influence Activities Course available by distance learning (60%) and resident learning (40%) by FY 13, realizing a \$500K/year in savings over the current fully-resident course model.¹⁶ Meanwhile, the JC4ISOC faculty is already reconstructing Classroom 236 to take advantage of online software like Blackboard in order to provide future JC4ISOC students a deeper learning experience.

Likewise, the (USD-P/I and JS J-39-sponsored) Joint Staff J-7's Training Needs Assessment (TNA) for IO and individual IRCs is vitally important toward improving and codifying joint IO training and education by identifying the joint IO professional's critical knowledge, skills and abilities (KSAs). Identifying gaps and seams isn't enough. The GCCs must support this effort to the same extent they have supported the USSTRATCOM Cyberspace Training Initiative.

Supporting this process is important for the JIOPC, which JC2IOS developed based on a 2005 TNA. While the 2005 TNA served the JIOPC students well, JC2IOS expects to revise and refine the JIOPC in FY 13 based on the 2012 TNA and impending joint doctrine updates. The JIOPC revision needs to consider blended learning for the previously mentioned IO basics for JCWS as part of future curriculum.

Simultaneously, JC2IOS continues to monitor the USSTRATCOM Cyberspace Training Initiative for potential opportunities to educate and train joint students on planning and integrating cyberspace operations, which may also include C4I systems planning and integration.

Conclusion & Recommendations

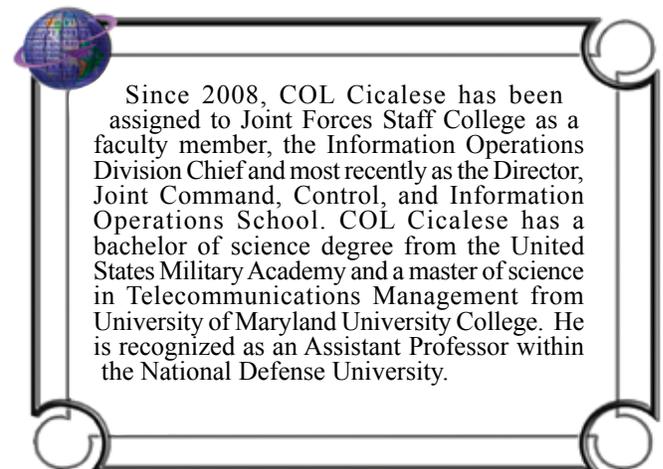
As the National Defense University prepares a mission analysis to center its main effort on the provision of JPME in the conduct of joint training, research, and outreach, and as the IO force prepares to identify the joint IO planner requirements for 2020, JC2IOS is uniquely poised to enhance JPME and joint training for operations in the IE. Just as it has done for the past thirty-three years, JC2IOS will harness its extraordinary faculty and proximity within the JFSC to optimize the joint student time and learning experience.

JC2IOS will continue to improve C4I and cyberspace training and education. It will update its IO curriculum based on the KSAs identified by the ongoing TNA. As a result, JC2IOS must assume leadership in identifying how to integrate requirements and courseware to fully utilize experienced faculty

and minimize student time away from the joint command. By doing so, JC2IOS can maximize the students experience while economizing resources.

Endnotes:

1. Dempsey, General Martin E. "Building Critical Thinkers." *Armed Forces Journal*. <http://www.armedforcesjournal.com/2011/02/5663450> (accessed February 16, 2012).
2. US Department of Defense. *Strategic Direction for the Joint Force*. Washington, DC: Chairman of the Joint Chiefs of Staff. 2012.
3. US Department of Defense. *Memorandum for the President, National Defense University (CM-0022-12)*. Washington, DC: Chairman of the Joint Chiefs of Staff. 2012.
4. US Army. "Army establishes Army Cyber Command." U.S. Army <http://www.army.mil/article/46012/army-establishes-army-cyber-command/> (accessed February 23, 2012).
5. Boyd, Colonel Curtis. "The Future of MISO." *Special Warfare 1* (January-February 2011): 22-29.
6. US Department of the Air Force. *Air Force Instruction 10-702, Operations*. Washington, DC: Department of the Air Force. 7 June 2011.
7. Congressional Research Service. *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*. Washington, DC: Government Printing Office, 2007.
8. Shanahan, Brigadier General John, N.T. "Information Operations in an Age of Shrinking Budgets: Crisis or Opportunity." *IO Sphere* (December 2011): 2.
9. Petty, CAPT (USN) Roy and Helm, CAPT (USN) (RET) Stephanie, "The Value of Graduate-Level Education to Information Operations." *IO Sphere* (December 2011): 21.
10. US Department of Defense. *Policy Directive 1(Draft)*. Norfolk, VA: Joint Forces Staff College. March 2012.
11. Shanahan, 2.
12. Vice Admiral Rodney P. Rempt, interview by Seth K. Powell, tape recording, Annapolis, MD, October 17, 2004 quoted in Powell, Seth K. "'Train for the Known, Educate for the Unknown: The Navy's Struggle for Clarity With Graduate Education in the Humanities, From Holloway To Rickover.'" *Undergraduate Thesis, United States Naval Academy, 2004*.
13. Drummond, Jonathan. "The Next Decade and Beyond: Foundational Force Development for a New IO." *IO Sphere* (December 2011): 10.
14. Shanahan, 2.
15. Dr. Robert Hill, interview by author, Fort Leavenworth, KS, February 23, 2012.
16. Dr. Robert Hill, interview by author, Fort Leavenworth, KS, February 23 2012.



JIOWC Transregional Conflict Prevention Initiative (TCPI) Optimizing the use of Information-Related Capabilities in a Budget-Constrained Environment

By
Mr. Richard Josten

Editor's Note: The JIOWC's approach to transregional and transnational issues is extremely important to the IO community. Future security issues will almost certainly have transregional and cross command implications. Creating a way of dealing with those aspects is essential to success in operations and conflict prevention. This is one possible approach to solving these complex problems.

History is not circular, but it is often repeated because we fail to learn from the past as we plan for the future. As the military enters into another post-conflict era of reduced spending and decreased capacity, our leadership seeks solutions for bridging gaps from capabilities to requirements. The current climate facing regional and functional combatant commanders (CCDR) requires a rebalancing for the future that makes it difficult to focus resources and attention on potential transregional threats. These challenges also make conflict-prevention information-related activities more necessary. In this climate, measures that obviate further military commitments, save money, and resolve tensions are a sound investment.

Historically, it has been difficult to maintain capability of forces during a drawdown. Faced with similar austerities and transregional challenges during World War II, Winston Churchill once declared; "Now that we are out of money, we need to think." Last fall, outgoing Deputy Defense Secretary William J. Lynn III warned in a keynote address to the Center for American Progress, that the U.S. is "0 for 4" in managing defense drawdowns. He also stressed that, "the Defense Department must reduce troop levels while retaining the ability to configure forces for emerging threats..." Reinforcing that perspective, Secretary of Defense Robert Gates, in his article in the November 2007 Issue of *World Politics Review* in the article titled "Radical Soft Power Proposal" said, "I am here to make the case for strengthening our capacity to use soft power and for better integrating it with hard power."

The Transregional Conflict Prevention Initiative (TCPI) is a process that identifies a means of bridging potential capability gaps and addressing current challenges to better utilize operations, actions, and activities (OAAs) in order to favorably shape the future strategic environment. With soft power and associated influence strategies, the U.S. has made strides at reducing the asymmetric advantage our adversaries have

***"However beautiful the strategy,
you should occasionally look at the
results." - Winston Churchill***

mastered in the information environment since 9-11. Many of those efforts to reduce adversary capabilities have focused on the tactical and operational levels, responding to the news cycle and the disinformation spread by adversaries into the traditional world media. TCPI is a process developed at the Joint Information Operations Warfare Center (JIOWC) to support shaping the information environment at the transregional level. The efforts of Rear Admiral Greg Smith, followed by those of Rear Admiral Hal Pittman within ISAF's strategic-communication effort, have shown the value of information-related capabilities (IRC) at the tactical and operational levels. The JIOWC interviewed both officers as part of the Strategic Communication Capabilities-Based Assessment (tasked by Joint Requirements Oversight Council on behalf of the Building Partnerships Functional Capability Board in 2010). Their success was due in part to the development of an information effects-based communications strategy and the inclusion of operational analysis. A key to the success of a communications strategy includes continuous tactical and operational assessment.

So what have we learned from a decade of war? One opinion from our British partners appeared in a new book, *Behavioural Conflict*, coauthored by Major General Andrew Mackay and Commander Steve Tatham of the British Army and Royal Navy respectfully. According to Maj Gen Mackay, "There's not enough emphasis on strategic communications, psychological operations, the role of persuasion and negotiation, and adapting the way we do things. Those have been cast to one side in favor of the purchase of an ever more effective weapon system or vehicle."¹

"And we will safeguard America's own security against those who threaten our citizens, our friends, and our interests," declared President Obama in the 2012 State of the Union Address. How is this possible in the face of a looming

IO Education and Training Catalog of Courses



Located on All Partners Access Network (APAN), the Joint Staff J-39 and J-7 (JCW) have sponsored the listing of IO Training Opportunities Available to the IO Community. View the catalog at:



https://community.apan.org/ioc/io_force_development_and_training/p/trainingandeducation.aspx
(Must Join APAN to View Catalog)

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

military drawdown? Historically, military drawdowns require a judicious review of national strategy to ensure security is not jeopardized. Subsequently, at the unveiling of the 2012 Strategic Guidance, Secretary of Defense Leon Panetta stated, “We must avoid hollowing out the force—a smaller, ready and well-equipped military is preferable to a larger, ill-prepared force that has been arbitrarily cut across the board.”

Based on the Obama Administration’s guidance, the primary security focus areas for the U.S. will rebalance from the Middle East to the Asia-Pacific region. This rebalancing during a post-conflict drawdown creates risk if transregional issues are not planned for correctly and may lead to lost opportunities. Continued focus of Department of Defense (DOD) resources on the Middle East also diminishes the availability of traditional military assets in the Pacific. Interestingly, using information as power to influence fits nicely into both the geo-strategic constraints and opportunities of the Pacific region. First, *employing the information element of power is relatively cheap*. Dr. Kristen Lord, of the Center for a New American Security, points out that the State Department’s use of public diplomacy to wield information as power is but a minute fraction of DOD’s budget. In addition, while it may seem counterintuitive to the uninformed to consider the US military as a source of ‘information-as-power’, in fact their influence by co-opting can be significant. Each CCDR develops a long-term strategy and campaign plan (with its imbedded theater security plan) for that very purpose. These strategies spawn military relationships and military-sponsored activities that send significant and loud messages to the populations of the region.²

Combatant Commanders must focus on commitments to their joint strategic capabilities plan’s (JSCP) assigned responsibilities, maintaining operational readiness and conducting required theater security cooperation plan (TSCP) activities. The downsizing of personnel, resources, and traditional lethal combat capabilities amid other severe

budget constraints and rebalancing exacerbates their resource limitations. Meanwhile, Lieutenant General Michael T. Flynn, Assistant Director of National Intelligence, puts it in the context that adversaries operate in a “multi-nodal threat environment” (NMS-2010), that is, “a threat construct exceedingly complex and adapting.” In essence, this approach calls for a greater use of soft power while maintaining credible forces with sufficient reach in a non-kinetic manner if kinetic options are not viable. LTG Flynn, also stated; “We need to focus on the precursors to war—as Secretary Gates said, ‘left of the boom’—to head off trouble before it explodes...Future conflicts will be hybrid asymmetric threats and global...transregional in nature.” LTG Flynn asserts that the cost of operations could be reduced through the use of conflict prevention Operational Activities and Actions (OAAs) as opposed to lethal means.³

As part of the Joint Staff (JS), JIOWC is postured to address transregional information-environment challenges in the current and future post-conflict arena. The JIOWC’s mission according to Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5125.01 is to “Support the Joint Staff in improving DOD’s 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.” Each regional combatant command (CCMD) has developed an information-related program of record designed to support end states and objectives stated in the theater campaign plans (TCPs). These programs are often called “Voice.” The operations are designed to coordinate and synchronize the CCMD’s influence activities, often tracking activities such as key-leader engagements with nations in their area of responsibility (AOR). JIOWC’s Integration and Assessment Teams, through planning and assessment support, assist in improving the process of capturing and assessing information activities. Since all activities are presented per CCMD, JIOWC



US Marines Hand Out School Supplies to Girls as Part of an Engagement Program to Counter Transnational Terrorist Influence

Source: defenseimagery.mil

can then help develop a transregional outlook, which is not limited to a single CCMD's AOR and has a transregional approach.

Guidance exists demonstrating the need for a transregional strategy, such as the TCPI process. The JIOWC is uniquely positioned to facilitate the planning of IRCs as a cost-effective means to achieve CCMD- and Joint Staff-desired effects. These effects are stated in strategic guidance documents such as the Defense Strategic Guidance, National Military Strategy (NMS), Guidance for Employment of the Forces (GEF), and TCP of individual CDRs.

Strategic Guidance - Global (Transnational/ Transregional) Security Challenges

Defense Strategic Guidance - Sustaining US Global Leadership: Priorities for 21st Century Defense.

This key strategy document released in January 2012, states that the U.S., its allies, and partners need to be capable of working in areas of anti-access and area denial (AA/AD) in the future, and that the DOD will encourage a culture of change to operate in these areas.

The 2012 Defense Strategic Guidance also states:

- Whenever possible, we will develop innovative, low-cost, and small-footprint approaches to achieve our security objectives, and
- The US military will invest as required to ensure its ability to operate effectively in AA/AD environments. This will include implementing the Joint Operational Access Concept.

Joint Operational Access Concept (JOAC), 2012.

There are several capabilities identified as essential to the implementation of the JOAC, two of which are specific to information and engagement:

- Information, JOA-027, is the “ability to inform and influence selected audiences to facilitate operational access before, during, and after hostilities.”
- Engagement, JOA-028, is the “ability to develop relationships and partnership goals and to share capabilities to ensure access and advance long-term regional stability.”

National Military Strategy, 2010

Key National Military Objectives (NMOs) that can be affected by IRC OAs are:

- Counter Violent Extremism
- Deter and Defeat Aggression
- Strengthen International and Regional Security
- Shape the Future Force

The NMS also addresses “Transnational challenges...Response to natural disasters and transnational threats such as trafficking, piracy, proliferation of weapons of mass destruction (WMD), terrorism, cyber-aggression, and pandemics are often best addressed through cooperative security approaches that create mutually beneficial outcomes.”

Guidance for Employment of the Forces, 2011

“This guidance also recognizes the global nature of several important emerging security threats. Countering these threats requires a high level of coordination and integration across



Secretary of the Army John McHugh Talks to Philippine Army Lt. Gen. Raymundo Ferrer about Operations in the Southern Philippines

Source: defenseimagery.mil

CCMD boundaries and across functional areas. ...Commands will identify the “out of theater” implications of the commands’ activities and coordinate as necessary with appropriate geographic and functional combatant commanders. Any given DOD operation or activity, although focused on a particular theater, could have global implications.”

“...properly applied IO is exactly what we need more of...” - Brig Gen John N.T. Shanahan

Over-the-Horizon (OTH) Emergent Issues

Our adversaries are not similarly limited by authorities that restrain traditional military operations because they are able to find asymmetric means to bypass traditional US military strength. CCDRs rarely have sufficient time, resources, and surplus capacity to devote to identification of “out of theater” (GEF-2011) effects of their command’s activities or toward shaping/conflict prevention activities that may be executed in one theater in order to create effects and/or achieve objectives in another. Transnational or transregional (including cross-domain as noted in the JOAC) challenges, though addressed in the NMS, GEF, TCPs, and other strategic guidance documents, often fall into the gaps and seams of CCMDs and thus are sometimes not thoroughly explored until those OTH issues transition beyond phase 0 and/or conflict prevention.

Shape (phase 0)— (i.e., *conflict prevention*) defined as: “Shape phase activities must adapt to a particular theater environment and may be executed in one theater in order to create effects and/or achieve objectives in another. ...CCMDs will nest phase 0 activities and tasks into the TSCP.”⁴ In December of last year, General Raymond T. Odierno, Chief of Staff of the Army, unveiled a concept that embraces both conflict prevention and

shaping called *Prevent, Shape, Win*. It includes shaping “the international environment so our friends are enabled and our enemies contained. We do that by engaging with our partners...”

Conflict prevention is defined as: “A peace operation employing complementary diplomatic, civil, and, when necessary, military means, to monitor and identify the causes of conflict, and take timely action to prevent the occurrence, escalation, or resumption of hostilities. Activities aimed at conflict prevention are often conducted under Chapter VI of the United Nations Charter. Conflict prevention can include fact-finding missions, consultations, warnings, inspections, and monitoring.”⁵

“The primary influence processes of information operations and strategic communication arguably work best in an environment where the U.S. hopes to shape the environment to support their interests while deterring aggression by potential adversaries (known as phase 0 and phase 1 operations in military terms)... Again, these are relatively cheap ways to influence compared to the enormous economic costs of hard power reflected by traditional military hardware and force structure.”⁶

While the Pacific will draw our attention, effects of the Arab Awakening and recent US operations in the Middle East will remain a salient issue well into 2020 and beyond. In his FY14-18, Integrated Priority List (IPL) submission, General James N. Mattis, Commander USCENTCOM, wrote: “Current combat and stability operations have proven costly. We continue to pursue high impact, cost efficient capabilities such as Counter Adversary Information Operations (CAIO) and Build Partner Capacity designed to promote stability and reduce the need for US military lethal operations. If hostilities erupt, military options will require a robust blend of lethal and non-lethal capabilities...” The commanding general identified CAIO as the number one capability gap to execute his assigned theater mission.



US Navy Adm. Mark Fitzgerald Speaks with Reporters on Efforts to Counter Piracy and Transnational Threats

Source: defenseimagery.mil

In previous edition of the *IO Sphere*, Brigadier General John N.T. Shanahan, Joint Staff J-39, wrote, “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.”

Earlier in this issue, Brig Gen Shanahan commented, “...properly applied IO is exactly what we need more of, when the rest of the big-ticket kinetic force is faced with hard times ahead.”

How is TCPI planning accomplished?

Now that we have established the need for the TCPI here’s how we do it. At the JIOWC, we have a Transregional Operations Planning Team (T-OPT) process standard operating procedure (SOP) based on the Military Decision-Making Process and the Joint Information Operations Planning Process. Who participates in the OPT? It depends. JIOWC J35-Strategic Plans and Integration may initiate the process based on an over-the-horizon emergent issue—either identified internally,

or nominated by a JS directorate, a CCMD or component, or an interagency or international partner. How do we determine the validity of a project? We use a simple six-step process from our SOP (see Figure 1). How do we measure success?—or how can we draw a conclusion that IRCs prevent conflict? First, effects from IRCs do not take place overnight, nor are they always easily traced to IRC OAs. It helps if there is already a baseline of data established for a given situation; if indicator data from polls, surveys, foreign media analysis and so on is not readily available, then it must be planned into the activity. Information/intelligence requirements should be considered up front—measures of performance and more importantly, measures of effectiveness for assessment need to be considered when planning objectives are established.

The focus of a TCPI plan is on the military and information capabilities within the diplomatic, information, military, and economic instruments of national power. During the TCPI process, a strategic planning seminar involving a community of interest/action (COI/A) may occur. One of the outputs of the seminar is to highlight and validate a specific OTH problem set for further

planning. Although the focus of the effort is on the military and informational elements of power, all elements are considered for engagement activities. If the *issue* is validated then a product of the further planning effort is an influence alert package (IAP).

For each validated trans-regional OTH *issue*, following a planning seminar, development of a COI/A, or the production of an IAP, the JIOWC may present the JS and CCDRs with a draft planning order, if tasked. The JIOWC can produce plans that contain pre-screened, pre-vetted, culturally aligned IO objectives, including initial target sets and proposed themes and messages. In our preparation for transition from USSTRATCOM to the JS, the JIOWC conducted approximately ten T-OPTs in as many months. The status of various T-OPTs and draft IAPs are briefed to the DDGO staff in person, via VTC, and via weekly update inputs. Any of the TCPI problem sets deemed worthy by the JS or a joint commander can be fully developed, as described in the preceding paragraph. “On-the-shelf” TCPI products can also be maintained and reviewed periodically for future use should OTH *issues* gain renewed interest (some already have).



JIOWC Transregional Conflict Prevention Initiative (TCPI) Process

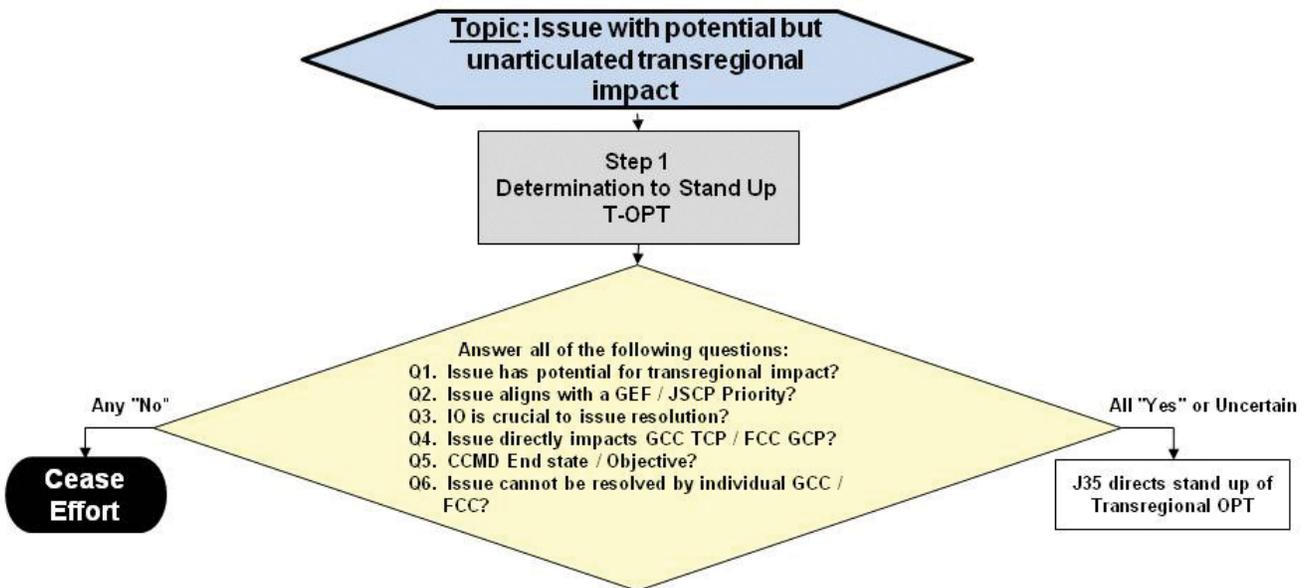


Figure 1. JIOWC TCPI Validation and Planning Process

TCPI Way Ahead

Given the current budget-constrained environment, the use of IRCs as a cost-effective means of achieving CCMD- and JS-desired effects is a logical course of action. IO OAs, as opposed to traditional kinetic OAs, offer an “economy of resources” means to achieving NMOs. Developed TCPI/IAPs directly address the JIOWC’s number one mission-essential task: operational support to the JS, military, Services, and DOD agencies to assist in coordinating and integrating DOD operational support for joint commanders.⁹ Furthermore, the products developed via the transregional planning process can contribute significantly to resolving CAIO USCENTCOM’s number one IPL, as well as IO-relevant IPLs from other CCMDs and multiple CCMD TCP objectives that have transregional influence. Additionally, the TCPI concept addresses several key concerns expressed in various recent speeches and articles by key leaders. Certain IAPs have been briefed to the intelligence community (IC); a PACOM-focused effort was met with considerable interest by IC entities and the National Counter Terrorism

Center during information exchanges in February and March of this year. TCPI was formally introduced to the Service IO Centers and USAR Theater IO Groups at the JIOWC-hosted IO Summit on 29 February 2012, interest level remains high and further coordination is expected at the next IO Summit preceding the World-Wide IO Conference in early October 2012. ●

Endnotes:

1. *Behavioural Conflict: Why Understanding People and Their Motives Will Prove Decisive in Future Conflict*, Andrew Mackay and Steve Tatham, Military Studies Press, 2011.
2. *Pacific Nation: Implications for Strategic Communication*, Dennis Murphy Professor Information Operations and/Information in Warfare, Air War College, 26 Jan 12.
3. *LTG Flynn, Strategic Multi-Layer Assessment Conference*, 29 Nov 11.
4. *Joint Pub 5-0, Joint Operation Planning*, 11 Aug 11.
5. *Joint Pub 1-02, DOD Dictionary of Military and Associated Terms*, amended

15 Jan 12.

6. *Murphy*.

7. “*Information Operations in an Age of Shrinking Budgets: Crisis or Opportunity?*,” *IO Sphere*, December 2011.

8. *JIOWC CONOPS*, 18 Nov 11.

9. *Ibid*.



JIOWC TCPI Concept of Operations (CONOPS)



JIOWC Support to the Joint Staff, Services, and DOD Agencies to:

- Identify IO relevance of potential transregional issues or events
- Facilitate or participate in transregional operational planning team (T-OPT) activities to determine if an issue or event has impact on transregional IO
- Advocate for GCC/FCCs to Joint Staff for IO-related T-OPT or Joint Planning Group issues or initiatives, and
- Coordinate and conduct IO senior planning seminars

Figure 2. JIOWC TCPI Concept of Operations

Change of Leadership at the US Marine Corps IO Center

Marine Corps Base Quantico, VA-(January 19, 2012) The Marine Corps Information Operations Center (MCIOC) conducted its first change of command ceremony (COC) at the National Museum of the Marine Corps 19 January at 1530. The transfer of command from Colonel James P. Gfrerer to Colonel Christopher L. Naler represented the continuing maturation of a new and growing operational capability within the United States Marine Corps.

The MCIOC has provided Information Operations (IO) related support to the Marine Corps and to forward-deployed Marine Corps Air Ground Task Forces (MAGTFs) since their official opening on 9 July 2009. From that time through to today, the MCIOC has established itself as the clearinghouse for the MAGTF Commanders and the Marine Corps to obtain full-spectrum Information Operations (IO) planning and Military Information Support Operations (MISO formerly, known as Psychological Operations or PSYOP) support. In addition to providing operational support, as the Marine Corps' Executive Agent for IO, the MCIOC has supported the development of IO through doctrinal writing and review, organizational support, training, materiel, leadership, personnel and facilities (DOTMLPF), and has enabled the integration of IO into MAGTF operations worldwide.

At the direction of senior Marine Corps leadership, the MCIOC was designated a command in August 2011. Colonel Gfrerer, the MCIOC's first commanding officer, pioneered efforts to integrate and execute IO across the Marine Corps. The large turnout for the ceremony, with representatives from the Office of the Secretary of Defense, the Joint Staff, Army, Navy, and Air Force, illustrated the operational impacts of the MCIOC under the leadership of Colonel Gfrerer.

The Presiding Official for the COC, Lieutenant General Richard T. Tryon, DC PP&O, not only recognized Colonel Gfrerer's contributions, but he also highlighted the true uniqueness of what the MCIOC brings to the fight. He went on to officially welcome Colonel Naler and his family to this extremely challenging and exceptional command. The MCIOC currently

has personnel and teams deployed in Afghanistan and with Marine expeditionary units. ●

Marine Corps Base Quantico, VA-(March 20, 2012) Sergeant Major Dwight D. Jones, newly posted Sgt. Maj. of the Marine Corps Information Operations Center, accepted the NCO sword from Col. Christopher L. Naler, and 1st Sgt. Timothy J. Chaplin was relieved aboard Marine Corps Base Quantico March 20, 2012, signifying the transfer of responsibility as the command's senior enlisted leader and advisor.

Colonel Naler, commanding officer of the MCIOC, hosted the Sergeant Major of the Marine Corps, Sgt. Maj. Michael P. Barrett, as well as a large and diverse crowd of commanding officers and senior enlisted leaders from across the services that included a number of Quantico tenant commands, the Joint Forces Staff College, the Joint IO Warfare Center, the Army's 1st IO Command, and the Military Information Support Operations Command.

"I want to thank you for the past three years that I have had the privilege of serving as your First Sergeant," Chaplin said. Addressing the Marines of MCIOC, he continued: "I came to work every day for you – I hope that you learned as much from me as I did from all of you. This has been the most rewarding and challenging tour of duty that I have had in my career."

Both Jones and Chaplin were present to welcome back a recently-returned IO Planning Team from Afghanistan, as well as to send off a combined MISO and IO team to attach to the 24th Marine Expeditionary Unit.

"I've learned a lot from 1st Sgt. Chaplin in a short time and I look forward to working with you all," Jones said. "As a young sergeant, I never would have had the opportunity to lead a team on a MEU staff – that says something about the caliber of Marines you are and the confidence our leaders have in you."

1st Sgt. Chaplin will join 1st Battalion, 5th Marine Regiment as a company first sergeant. ●



Marine Corps IO Center Change of Command Ceremony at the National Museum of the Marine Corps

Source: MCIOC

A Match Made in Cyberspace

Secure Function Evaluation in Military Planning

By

Lieutenant Colonel Gerald R. Scott, US Army

Editor's Note: LTC Scott's discussion in this essay is very important to the concept of information integration in a secure planning system. Securing military information has always been an issue in the history of warfare, but with the proliferation of information technology it is even more pronounced.

Substantial effort has been put toward intelligence and operations integration over the past decade with significant progress made, particularly for conventional operations and special operations. Integration for information and technology operations¹ has also improved, but has not equaled the integration in other areas. Additionally, and possibly more important for information and technology operations, is the integration of both policy and capabilities into the operational construct. This paper describes the relationship between these four areas of information and the challenges of integrating them in a secure environment, and proposes some potential solutions that could be used to improve integration.

Military planning activities can be described as involving four areas of information: intelligence, planning and execution, capabilities, and policy. For conventional operations, capabilities and policy typically don't get specific attention because they are less dynamic than the other two. Capabilities for conventional operations have been developed over years and are typically well known to the forces prior to the operation. Over the past several years, rapidly fielding programs such as the one developed for the Mine Resistant Ambush Protected vehicles have changed this somewhat; however, from the operational planning perspective, capabilities remains a relatively constant, known factor. Policy has similar features for

conventional operations. For example, the debate and decision to go to war is generally public and deliberate. A policy may not be decided until late in a crisis, but once it is, it is relatively clear and understood by all those involved.

For information and technology planning, these areas may be much less defined. Capabilities may be still in development while an operation is being planned, custom built for a single mission, or not fielded to the entire force. Similarly, policy discussions may be limited to a very select group of senior leaders, decisions may not be shared with the operational force, and specific policy decisions may have to be made regarding the use of certain capabilities such as cyber-attack tools. The smooth integration of information in these areas is therefore more challenging for information and technology planning. Security of these operations is often more critical and so the challenge of integration becomes compounded by classification and compartmentation.

Classification and Compartmentation

Effectively using information protected by multiple classifications and compartments is a significant challenge faced by planners.² If all information were at a common classification, the matching of capabilities to effects would be a relatively simple task (data availability and processing large amounts of data present their own challenges, but multi-level security compounds these challenges.)

Information may be classified and compartmented in all four informational areas discussed here. Information regarding capabilities may be held within proprietary channels, or the technology may be government developed and protected in a limited-access compartment to prevent adversaries (and potential adversaries) from developing like technology or from developing counter measures. Policy information may similarly be limited to a very small circle to protect the government's ability to negotiate with other countries or to hide intent. Intelligence information may be classified or compartmented to protect sources and methods from disclosure, and planning information may need to be compartmented to protect on-going or future operations or to protect tactics, techniques and procedures. The challenges planners face due to classification and compartmentation are further compounded in a coalition environment in which the participating countries want to contribute to the whole, but have a requirement to protect information from other members of the coalition.

The challenges of integration in a classified and compartmented environment can be visualized as a simple bull's eye as depicted in figure 1 (page 35). Outside the red circle, in the unclassified realm, there are challenges to the integration of the four areas of information. These include the storage of data that is not discoverable, and other well-known barriers to effective coordination. Inside the red circle, in the classified environment, these barriers are significantly increased because not everyone is allowed to access the information; however, information exists on networks that do not communicate readily with each other, and additional means of secure communication



Former Deputy Secretary of Defense William J. Lynn III
Speaks at the 2010 Cyberspace Symposium
Source: defenseimagery.mil

may not be available across or outside of the network. Inside the orange circle, in the compartmented realm, the barriers are increased yet again, as specific by-name access may be required for access to information. Information can only be handled in specific designated areas, networks may be deliberately designed to keep information from being discoverable, and a deliberate justifiable culture of “need to know” vs. one of “need to share” has been maintained.

These challenges apply to all four areas of operationally relevant information, and while there are recurring, and often legitimate, claims of over-classification and compartmentation, it would not be prudent to force information and technical-related planning to take place at a common classification. Doing so would put one or more areas of information at risk. No category of information is *prima fascia* more important to protect than any other information category; it is important to protect all of the information while making the best possible use of the

information as a whole. Current practices, however, actually favor the protection of information related to capabilities over information regarding the planning or operation that will be the focus of the remainder of this paper.

A growing challenge for the information- and technology-focused military planning community is the matching of technological capabilities with desired effects in support of a military plan or operation. While always a challenge, it has become more complicated for a number of reasons; for example, the aforementioned classification and compartmentation issues, current procedures for identifying a capability to achieve a particular effect, and the drivers of technological innovation.

Current Procedures

Planners use a variety of procedures to help identify what capabilities are available to achieve desired effects, along with numerous procedures to help capability developers identify

what effects are, or will be desired. In general, throughout the information- and technology-focused military planning community, the procedures follow a pattern. The planner is required to express with significant detail and precision what effect is desired, then the planner releases this information to an amorphous community of capability providers for analysis. A capability provider then replies with their capabilities that can best achieve the effect, or replies that they have no capability that can achieve the effect without providing any additional insight to the planner.

There are three primary shortcomings in the current process:

1. The capability provider has the ability to withhold information for reasons not related to the request (i.e., funding, competing requirements, etc);
2. The planner/requester may be forced to disclose sensitive information regarding the operation in order to determine if a capability is available, and;

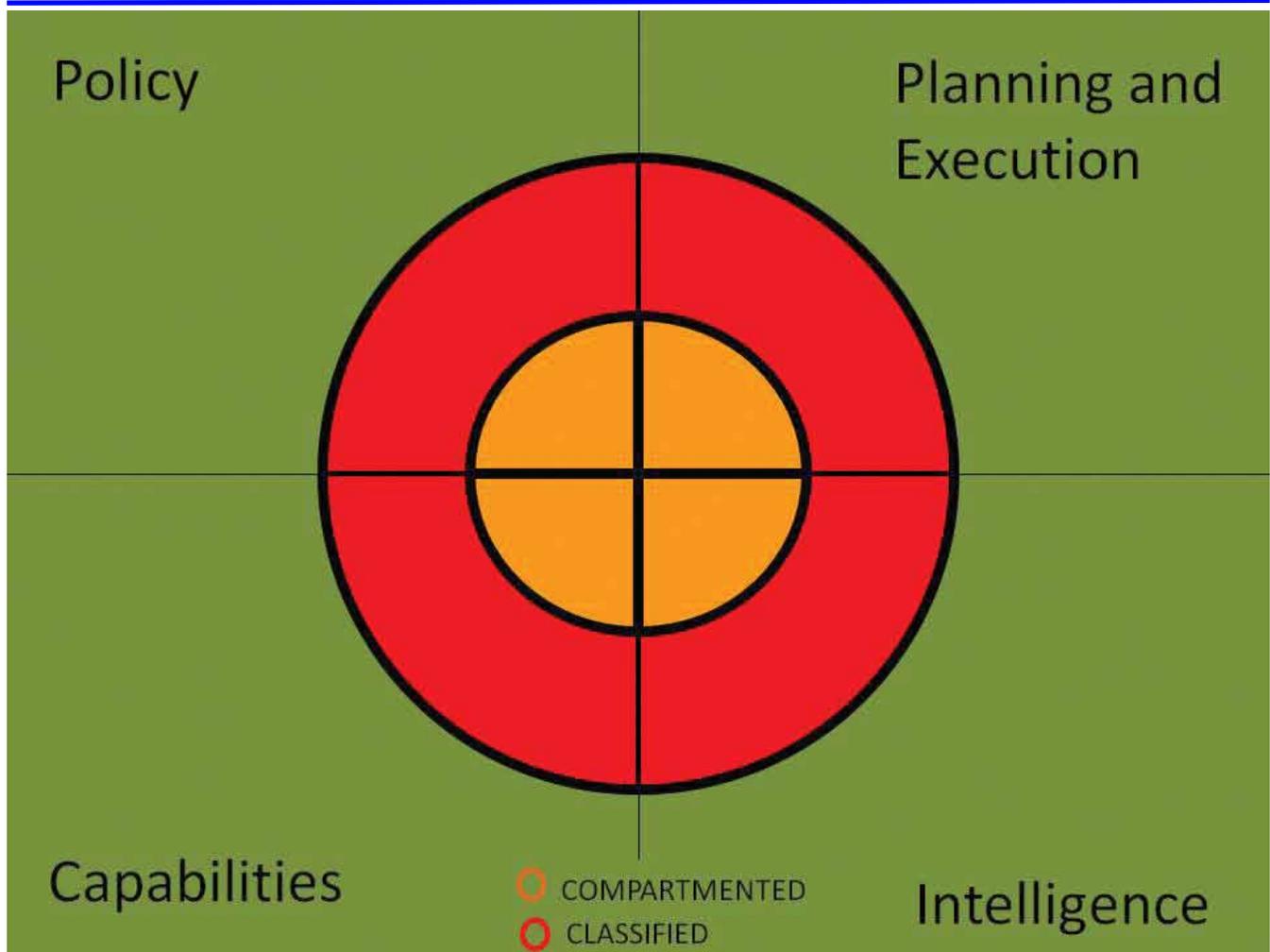


Figure 1-Barriers to Integrating Information in a Classified Environment

3. The planner may not identify a desired effect because he has no knowledge that a capability exists that may be able to achieve the effect.

To overcome these shortcomings, a cadre of experts has grown within related communities to help the system work. The “Bubba-net” or “*Shadchonim*”³ of the technical planning world are typically widely briefed into programs and compartments from all four areas of information and serve as a primary point of contact for military planners who may not be able to share planning details widely. This informal practice helps to overcome the friction in the current system, but it has drawbacks. *Ipsa facto*, it is haphazard and may not produce a match when one is available. Additionally, there is no mechanism to ensure that the match that is developed is the best possible match of capability to requirement. Finally, it creates a security risk by concentrating large amounts of sensitive information across all four areas of information in individuals, albeit trusted individuals.

Drivers of Technological Innovation

The pace of technological innovation in the commercial sector has eroded what was once the government’s monopoly on military-applicable technology. The military now lacks a coherent and comprehensive source of information regarding what technology may be applicable to a particular situation. This is due, in part, to the inability to classify or compartment a technology that is being developed without government funding, as well as the result of commercially developed technology not being clearly aligned with the functional military community where it might be applied. This has limited the ability to match capabilities with desired effects when the best capability either is outside of a narrowly defined community of expertise (e.g., electronic warfare, or intelligence, surveillance, and reconnaissance) or is not currently in the military inventory.

This is particularly evident in regard to information and non-kinetic capability development. With technologies that are designed to produce a kinetic or clearly military effect, the military is the sole, or at least a primary, market for a development company. However, with certain information technologies, the military is a secondary market, or sometimes not identified as a market at all. In these cases, the military is often deficient in its understanding of the “realm of the possible.” Instead of military necessity driving technological development, technological developments have the potential to drive military opportunity, but only if those technologies are accessible, both conceptually and physically, to the planning community.

Similar Information Problems and Solutions in Industry

These problems are by no means unique to the military. Indeed, many information-related businesses face similar problems and can be used as a model for developing military solutions. Internet dating services, medical records analysis, and online banking all provide insight into solutions that the military may be able to implement in the planning environment.⁴

Internet dating seems an unlikely field to provide a military solution, but from an information management and security viewpoint, it looks remarkably similar to the matching of capabilities to requirements. First, the general problem set of finding a match in a changing world, the use of matchmakers is no longer an effective way of finding a match except in very limited cases that is the primary driver for the entire business area

of internet dating. More importantly, the information-security issues are similar. A person using an internet dating service should not want to put all of his or her private information in a public forum for others to view with no regard for security – the risks are obvious. Successful companies develop mechanisms to both protect private data and use that data to find potential matches. The most successful of them are able to go a step further and ensure that users’ private information is not even accessible to company insiders, a key security aspect of the system that would benefit military applications.

One frequently raised concern regarding the development of information management systems for classified data is the administrative overhead associated with managing the system. Many security policies require persons with access to the classified information to have a “need to know” the information and are required to provide some material contribution to the effort based on their knowledge of the information. It is often hard to justify giving additional personnel access to the information for the sole purpose of managing the information system where the data resides. By studying the practices of Internet dating and similar companies, the military could design systems that limit the ability of IT administrators to access sensitive data, allowing for more robust data sets to be compiled without increasing the risk of disclosure. It would provide a means to increase the flow and utility of information without increasing access to the information and the risks associated with increased access.

Medical and education records management and distributed data mining also provide insights into how the military might design better systems. Medical and education researchers face a key challenge in balancing the analysis of data with the privacy rights of patients, students, doctors and teachers. As more and more records are digitized, the ability to analyze the effect of drugs or procedures over time and across large populations has increased exponentially. Instead of conducting a limited trial, researchers now have the technical ability to create a virtual trial using all the recipients of a drug or procedures since its first use. However, they are prevented from doing so because the researchers would have to gain the consent of all of the involved parties. Medical providers and school districts in particular are not inclined to open their records to such research because they open themselves up for malpractice accusations or other liability concerns.

To overcome these policy-driven challenges, researchers are developing methods so that only statistical information not associated with any particular patient or student is transferred out of their control. The researchers develop algorithms and queries that can be run against a privacy-protected database. The results are then securely compiled with other results and transferred to the researchers. A similar procedure could be used to analyze after-action reviews and lessons learned from sensitive operations in order to improve the performance of the force as a whole without disclosing classified information to those without a need to know.

Online banking operations need to protect access to personal records and the ability to manipulate the information contained in those records. However, in order to succeed in a very competitive environment, they need to provide easy access to legitimate customers and facilitate smooth, rapid transactions between a wide variety of customers and merchants. In order to balance these requirements, the Internet banking system has developed a broad, interconnected system of verification and authentication using techniques that allow, for example, a customer to prove to a merchant that her bank account has



Joint OPSEC Support Element (JOSE)



Program Development & Training Support Operations Security Course Schedule

Dates	Location	Course/Status	Seats
11-14 Jun 12	Ford Island, HI (PACOM)	OPSE-2500	30 Seats
18-22 Jun 12	Djibouti, Africa (Camp Lemonnier) (AFRICOM)	OPSE-2500 & 1500	30 Seats
17-20 Jul 12	Qatar (AFCENT HQ FWD) (CENTCOM)	OPSE-2500	30 Seats
30 Jul - 3 Aug 12	Dongducheon, South Korea Camp Casey (USFK) (PACOM)	OPSE-2500 & 1500	30 Seats
20-24 Aug 12	San Antonio, TX (JOSE) MacAulay-Brown Inc. Facility	OPSE-2500 & 1500	26 Seats
20-24 Aug 12	Fussa, Japan Yokota AB (USFJ) (PACOM)	OPSE-2500 & 1500	30 Seats
24-28 Sep 12	Grafenwoeher, Germany USAG Grafenwoeher (EUCOM)	OPSE-2500 & 1500	30 Seats
15-19 Oct 12	San Antonio, TX (JOSE) MacAulay-Brown Inc. Facility	OPSE-2500 & 1500	26 Seats
15-19 Oct 12	Daegu, South Korea Camp Henry (USFK) (PACOM)	OPSE-1500 & 2500	30 Seats
3-7 Dec 12	San Antonio, TX (JOSE) Fort Sam Houston	OPSE-2500 & 1500	26 Seats
4-8 Mar 13	San Antonio, TX (JOSE) MacAulay-Brown Inc. Facility	OPSE-2500 & 1500	26 Seats
22-26 Apr 13	San Antonio, TX (JOSE) MacAulay-Brown Inc. Facility	OPSE-2500 & 1500	26 Seats
3-7 Jun 13	San Antonio, TX (JOSE) MacAulay-Brown Inc. Facility	OPSE-2500 & 1500	26 Seats
11-17 Aug 13	San Antonio, TX (JOSE) MacAulay-Brown Inc. Facility	OPSE-2500 & 1500	26 Seats

Contact the JIOWC Joint OPSEC Support Element
Phone Number 210-977-5192 or 5650 (DSN 969)
Email at jiowc.jose@us.af.mil

the required funds for a transaction without disclosing any additional information about either the customer or the account itself.

The means used to implement the security practices in these services is fundamentally based on the cryptography concepts of secure function evaluation, specifically zero-knowledge proofs and privacy-protecting distributed data mining. For a simplistic example of secure function evaluation, imagine a coalition planning environment where members of the coalition are willing to contribute forces to an operation, but are unwilling to commit openly unless they know that the combined total of forces will be enough to accomplish the mission. They need a means to add up the total number of forces, without any party knowing any other party's numbers. This computation takes place in a series of closed (secure) computations and open transactions between the parties. These transactions are detailed in figure 2 (page 39).⁵

A zero-knowledge proof is a type of secure function analysis for one party to prove something to another party without revealing key, private information – essentially the mathematical equivalent of a double-blind live demonstration of a capability. Privacy-protecting distributed data mining is designed specifically to protect information within a database while allowing analysis to be conducted on the data and the results to be released. A concrete example of privacy-protecting distributed data mining is the use of multiple medical record databases to compile statistically relevant information about the transmission of diseases while protecting private patient information and information about the practices in any particular hospital.⁶

Similar techniques as those used to add numbers securely could be developed to address many military planning information requirements, in particular the matching of capabilities to desired effects. The problem of securely evaluating equivalence is generally referred to as the “Socialist Millionaire Problem”; that is, can two wealthy people determine if they have the same net worth without either disclosing their actual net worth?⁷ A secure function evaluation system for matching capabilities to effects would include a privacy-protecting distributed data mining capability to develop coherent sets of native data for both capabilities and effects that could then be processed using an iterative millionaire problem protocol to determine equivalencies between a large number of parameters and produce the most likely matches.

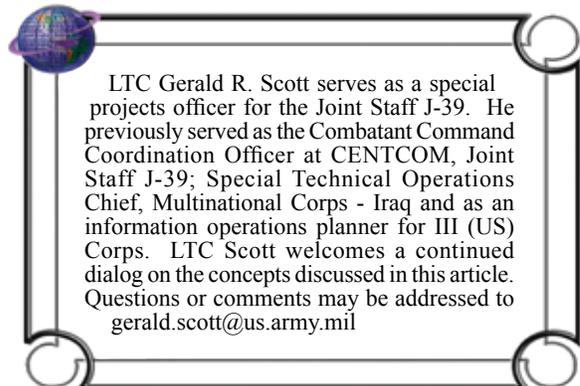
There are numerous networks within the Department of Defense that could be used to demonstrate these techniques and the improvements they may provide. Some of these networks are already isolated and protected in a way that would directly support the development of the software and procedures envisioned here. Efforts to develop these techniques should be pursued on a number of networks and include not just the technological development, but also propose changes to military policies and procedures.

Perhaps the next step in improving the military's ability to coordinate information across platforms and classification should be to develop an information-sharing protocol and data structure that would allow for a secure, distributed data-mining algorithm to facilitate an improvement in matching capabilities to requirements. Such a system would be relatively inexpensive to design, build, and implement and has the potential of providing a significant improvement over current practice. The military utility of other aspects of secure function analysis, however, is likely to be far broader than this proposal and, while

likely already used in numerous specific military applications, should be investigated for its broader utility in the information and technology operational areas. ●

Endnotes:

- 1. The term “information and technology operations” is a cumbersome, but useful, term to refer to the target audience of this paper. Other terms, such as “Information Operations,” “Influence,” “Cyber,” “J-39,” “ISR,” “Influence,” “Special Technical Operations” or others could be substituted but are neither inclusive nor precise enough for this purpose. The author intends to address the challenges faced by those military planners that do not work in the “conventional” operational environment, but are asked instead to develop innovative, alternative or supporting plans to achieve particular ends through information and technical means.*
- 2. For the purposes of this paper, it is not necessary to understand the specifics of the US military classification system—a discussion that would make this paper itself classified. From an information-management perspective, it is only necessary to understand that any piece of information might be both classified (broadly tiered levels of access) and compartmented (available only to specific individuals).*
- 3. Many cultures have relied on matchmakers as a key function of the society. As an example, Shadchonim is the Hebrew term for the professional matchmaking class within orthodox Jewish communities. The traditional practice of matchmaking or “Shidduch” bears a striking resemblance to the matching of military technologies and effects in the modern planning community. [<http://en.wikipedia.org/wiki/Shidduchim>] The term is particularly apt for this article as the proposed solution uses techniques that are also used by modern dating services such as eHarmony, which are replacing the Shadchonim.*
- 4. For a discussion of these practices, see “The Future of Privacy,” Scientific American. September, 2008.*
- 5. This example is based on and mathematically equivalent to an example in “The Future of Privacy,” Scientific American. September, 2008.*
- 6. “Privacy-preserving Distributed Mining of Association Rules on Horizontally Partitioned Data” Murat Kantarcioglu and Chris Clifton, IEEE Transactions on Knowledge and Data Engineering, Volume 16 Issue 9, September 2004.*
- 7. For a complete description of the socialist millionaire problem and other similar concepts of secure function analysis, see http://en.wikipedia.org/wiki/Socialist_millionaire.*



Secure Function Analysis Example

- All countries agree that 2250 is the minimum number of troops required in order to conduct this mission.

- Each country privately decides how many troops it is willing commit (A, B, C)

- In order to prevent any other country from deriving one of these numbers, each country add an agreed-to number (a modulator, in this case 1000) to their commitment. (A_M, B_M, C_M)

- Each country then picks three numbers that together add up to their modulated commitment. ($A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, C_3$, etc)

- Each country keeps one of the numbers private and gives one of the other two numbers to each of the other countries so that each country knows all of their own numbers and one number from each other country. Each country then totals their one private number with the numbers provided by the other countries so that:

- All countries then share their totals, add them up and remove the total of the modulators

- In this example there are not enough troops committed, but no country is able to determine for sure what any other country was willing to commit. The analysis could continue in this fashion in an auction format until the required commitment is reached.

Forces Required (T) = 2250

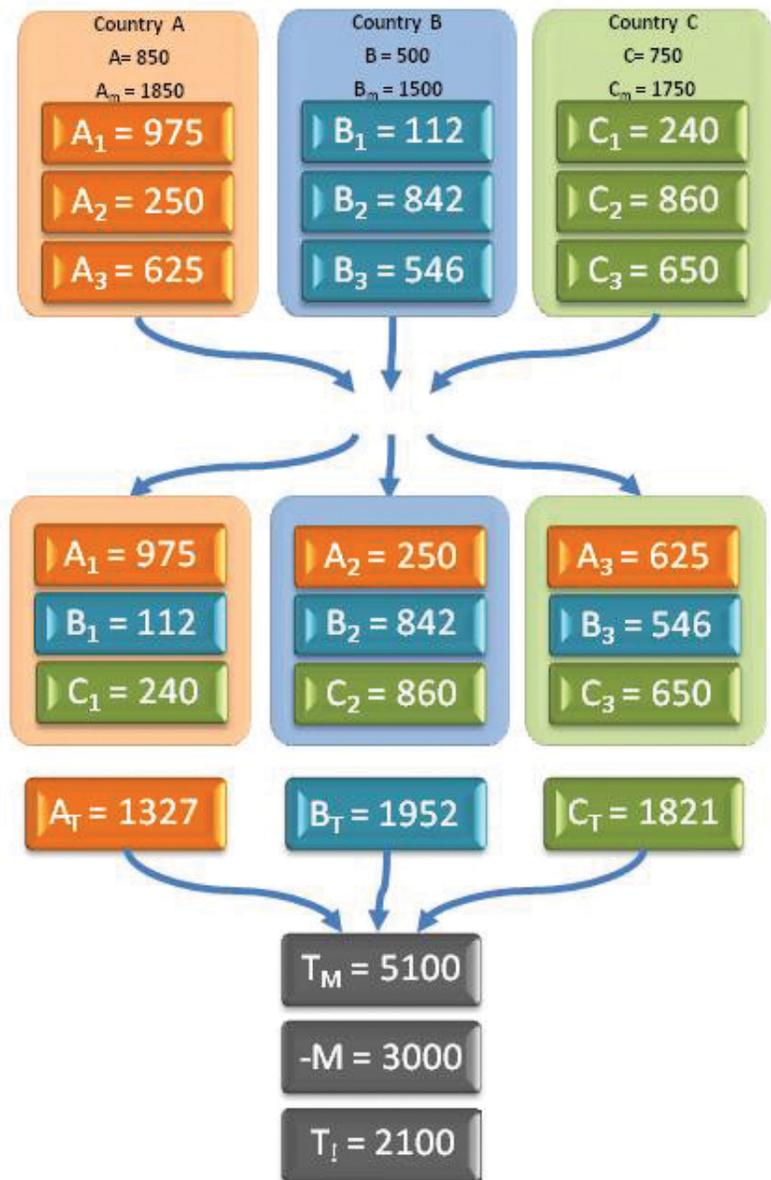


Figure 2-Secure Function Analysis Example

IO SPHERE

GENERAL CALL FOR ARTICLES

Become a Contributor

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

Published Quarterly 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. Also, all items should be security screened, and released by author's parent command/agency/organization/company prior to submission. Please include a letter or email documenting these actions.

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



IO SPHERE: 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 (4 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"

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

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

FOLD BACK HERE

OFFICIAL BUSINESS

PLACE
POSTAGE
HERE

JOINT INFORMATION OPERATIONS WARFARE CENTER

ATTN: IO SPHERE EDITOR / J55 Advocacy Branch

2 HALL BLVD STE 217

SAN ANTONIO TX 78243-7074

May 2012



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

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



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