AMERICAN INTELLIGENCE JOURNAL

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS

Intelligence Reform and Transformation

NMIA

Vol. 29, No. 1, 2011

American Intelligence Journal

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS

Vol. 29, No. 1 *2011* ISSN 0883-072X

The *American Intelligence Journal* (*AIJ*) is published by the National Military Intelligence Association (NMIA), a non-profit, non-political, professional association supporting American intelligence professionals and the U.S. Intelligence Community, primarily through educational means. The Board of Directors is headed by Lieutenant General James A. Williams (USA, Ret), and the president of NMIA is Colonel Joe Keefe (USAF, Ret). NMIA membership includes active duty, former military, and civil service intelligence personnel and U.S. citizens in industry, academia, or other civil pursuits who are interested in being informed on aspects of intelligence. For a membership application, see the back page of this *Journal*.

Authors interested in submitting an article to the *Journal* are encouraged to send an inquiry – with a short abstract of the text – to the Editor by e-mail at <William.Spracher@dodiis.mil or spracherw@yahoo.com>. Articles and inquiries may also be submitted in hard copy to Editor, c/o NMIA, 256 Morris Creek Road, Cullen, Virginia 23934. Comments, suggestions, and observations on the editorial content of the *Journal* are also welcome. Questions concerning subscriptions, advertising, and distribution should be directed to the Production Manager at <Admin@nmia.org>.

The *American Intelligence Journal* is published semi-annually. Each issue runs 100-200 pages and is distributed to key Government officials, members of Congress and their staffs, and university professors and libraries, as well as to NMIA members, *Journal* subscribers, and contributors. Contributors include Intelligence Community leaders and professionals as well as academicians and others with interesting and informative perspectives. Back issues of the *AIJ* are available to members within the U.S. at the cost of $25; to non-members and international requestors at $50.

NMIA CORPORATE MEMBERS

Accenture
Advanced Technical Intelligence Center
American Military University
American Systems Corporation
ANSER, Analytic Services, Inc.
Battelle Memorial Institute
CACI
Cobham Analytic Solutions
Computer Sciences Corporation
Concurrent Technologies Corporation
DynCorp International
General Dynamics Advanced Information Systems
Henley-Putnam University
JB&A, Inc.
KMS Solutions, LLC
L-3 Communications
Liberty University
Lockheed Martin, IS&GS, Global Security Solutions
Parsons Infrastructure & Technology Group, Inc.
Northrop Grumman Corporation
Pluribus International Corporation
Riverside Research Institute
Science Applications International Corporation (SAIC)
SOS International, Ltd.
Sytera, LLC
The SI
TAD PGS
Textron Systems
USGC, Inc.
Zel Technologies, LLC

AMERICAN INTELLIGENCE JOURNAL

Table of Contents

Table of Contents *(Continued)*

PRESIDENT'S MESSAGE

Welcome to the latest version of "Intelligence Reform and Transformation," the theme of this American Intelligence Journal (AIJ), and subject matter most long-timers believe we see coming up way too often. However, no matter how much "reorganization" makes you shiver, you will find this edition of AIJ a good one. Reform, Transformation, Reorganization, Change, Fix-It, New Mission – all are constants in our discipline. That is partially the nature of the business we do, with consistently changing priorities, threats, politics, consumers, and masters. It is also the result of the constant change factor built into "military intelligence" – new technologies, new systems, staff rotations, new leaders, etc. This issue is "good" not just because of the outstanding individual articles, the diversity of topics and viewpoints, or the intellectual insights of the authors. What makes this issue so valuable and interesting is that the sum total of the articles is an excellent primer on the state of Military Intelligence. The identification of problems in our discipline, the drivers behind them, potential solutions, political realities, and specific examples when added together provide an insightful tour of the realities of today's Military Intelligence discipline. The majority of the articles are also a "good read" and I hope you find them as interesting and thought-provoking as I did. Download this issue of the AIJ onto your Kindle and take it to the beach!

The National Military Intelligence Association and Foundation held the annual National Military Intelligence Awards Banquet in May with several hundred attendees honoring the best in Military Intelligence. Nineteen of our nation's finest intelligence professionals were recognized by NMIA/NMIF and their parent organizations. They ranged in grade from E-3 to 0-6 and included four intelligence civilians, with awards given to personnel from the Army, Navy, Air Force, Marine Corps, Coast Guard, National Guard and Reserves, and the national intelligence agencies. Also attending were the directors or deputies for these intelligence organizations/units. If you want another source or insight into what is happening in today's Military Intelligence discipline, please attend next year's banquet. The individual recognition provided by these annual awards is a keystone of the Association/Foundation charter. The accomplishments of these intelligence professionals and heroes have had an obvious and measurable impact on our nation's security. We are proud to be a part of that recognition process.

We have a couple of NMIA events coming up that I would like to highlight briefly. In August, NMIA is jointly sponsoring a conference in the DC area with the Association of Old Crows (AOC) on "Intelligence Electronic Warfare (EW) Operations." The objective is to help the EW community, operators, system developers, and intelligence community at large better understand the requirements, priorities, processes, and resources to enhance the EW mission over the next ten years. This is not just an informative or educational event. It is meant to be a 360-degree look at all things EW with all of the stakeholders getting to walk in the "others' shoes" and hopefully advance the overall EW mission. Check our website (www.nmia.org) or the AOC website (www.crows.org) for details.

The NMIA Fall 2011 National Intelligence Symposium is shaping up to be an outstanding event focused on "Small Unit Intelligence." Small units are the foundation of all direct actions conducted by military, law enforcement, public safety, and disaster management organizations. These units must acquire and process information and intelligence to determine their specific situations, and to establish a common operating picture within and among their units and their command and control hierarchies. They must apply information and intelligence to find and fix their "targets" and engage or prosecute them. Finally, they must create and report information for peers and superiors as they complete missions, recover, reconstitute, and prepare for the next engagement. We propose organizing and conducting a two-day symposium at the unclassified/unlimited distribution clearance level to discuss how intelligence and information activities can better meet the needs and requirements of small units. We also hope to better understand how leadership, organization, and training of small units may impact the collection, processing, and use of information. We want to better understand how the individuals and units at the "business end" of small unit operations provision and use intelligence and information to conduct their operations today, and how changes in information content, information delivery mechanisms, organization, training, and leadership could make them more effective in the future. The symposium will be held in the DC area in early November 2011. The symposium has been receiving a lot of interest during the building phase, and it will be difficult to fit all of our desired scope and content into two days. Major General (Promotable) Mike Flynn (ISAF/J2 and ODNI designate), Brigadier General Gregg Potter (Commander, U.S. Army Intelligence Center of Excellence), and several others who have a reputation for focus on the pointed end of the spear have agreed to participate in this event. Updates and details will be available on our website shortly.

NMIA would like to have you more active in the Association and, if you live in the Washington area, you have the opportunity to help resurrect the local chapter of NMIA (formerly Potomac, likely to be called the National Capital Area Chapter in the future). Our NMIA Chapters Chair, Cal Carnes (callandcarnes@cs.com), is leading an effort to get the chapter active again and to offer a series of

events of interest to our membership, to include a broader cross-section of our community who may not be able to attend our classified symposia. Please contact Cal if you have interest and a bit of spare time.

Well, this is the edition of the Journal where your Association goes digital. We are hopeful that over time the digital editions will help us to improve the flexibility and impact of the content, the volume of articles, and reduce the printing and mailing costs. In turn, that will allow NMIA to put more of its resources into other efforts that will meet the needs of the membership, such as symposia, scholarships, etc. If you have any observations, comments, or recommendations, please let us know – we value your feedback.

Joe Keefe

Interested in publishing an article in the *American Intelligence Journal*?

Submit a manuscript for consideration to the Editor
<spracherw@yahoo.com>

Welcome, loyal *AIJ* readers, to the first-ever issue to be disseminated to NMIA members principally in digital format. This was a decision taken by the Board of Directors to avoid excessive printing costs and bring us into the 21st century of "paperless" technology. Many other scholarly publications have gone this route and are taking similar measures. Nevertheless, a limited number of paper copies will still be available on demand. A few libraries may still want a paper copy (like the John T. Hughes Library here at the DIAC, where a copy sits on the periodical shelf and is regularly thumbed through by DIA analysts, NDIC students looking for thesis/term paper ideas, and instructors trying to stay ahead of them). Moreover, our growing stable of authors, some of whom are not yet NMIA members for unfathomable reasons, deserves to receive a complimentary copy or two when they contribute their thoughts and ideas in writing. For questions about obtaining hard or soft copies of *AIJ*, contact Deb Davis at admin@nmia.org.

The overall theme of this issue is "Intelligence Reform and Transformation." Over the decades, there have been countless studies completed and commissions formed to figure out how to "fix" what's wrong with the Intelligence Community. Many of their conclusions and recommendations have tread over the same old ground, suggesting reforms to counter the previous reforms and sometimes creating the perception that history merely repeats itself and offers lessons learned that are too quickly forgotten. Then again, more often than not, the calls to reform the IC, or fundamentally transform it, come on the heels of an "intelligence failure" such as Pearl Harbor, 9/11, or missing WMD in Iraq. As notable examples of previous calls for reform, in 2003 the late LTG (Ret) Bill Odom, former Army intelligence chief and NSA Director, wrote *Fixing Intelligence for a More Secure America*, and MG(P) Mike Flynn and associates stirred up a hornet's nest with their January 2010 monograph "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," published by the Center for a New American Security. This provocative piece by Flynn, just confirmed for promotion to LTG and a billet in ODNI dealing with partner engagement, is referenced by a couple of our present authors.

To provide some historical perspective to all the reform and transformation efforts, I commend to you a promotional brochure produced in 2007 by the Office of the Director of National Intelligence, titled "Six Decades of Intelligence Reform." The then-ODNI Historian (now Command Historian of U.S. Cyber Command), Dr. Michael Warner, introduced the brochure this way: "All of the 100-day focus areas represent complex problems that have long impeded Intelligence Community (IC) planning and operations.

Some have deep roots in IC institutions and practices, as shown by studies and proposals dating back in cases to the 1940s. Others are comparatively more recent, but all have been considered for years by advisory panels and blue-ribbon commissions. Since at least 1996, moreover, Presidents, Congresses, and senior decisionmakers have debated these issues in terms remarkably like those we have used to describe them today." At the end of the document, Warner lists 17 principal studies conducted by cleared and knowledgeable observers appointed by the White House, Congress, or the DCI to survey the functioning of the American intelligence system. To show just how pervasive the desire to reform or transform the Community has been, Warner observes that "Studies of the IC began almost as soon as the ink was dry on the National Security Act of 1947, which created the modern intelligence system in the United States."

In a perceptive September 2010 essay titled "'Changing Our Minds': Intelligence Reform Has Neglected the Cognitive Dimension – That Must Change," submitted for the IC's coveted Galileo Award, Josh Kerbel asks the question: "How does the IC open itself to the type of creative/imaginative thinking that 'breaks the rules' of linearity by being more associative, generative, integrative, and synthetic—more holistic—in nature? Due to an emphasis on bureaucratic, technological and misguided cognitive emphases on critical—vice creative—thinking, this is a question the IC is yet to adequately address." I for one have heard much about *critical thinking* in recent years; yet, *creative thinking*, which is harder to do, garners less attention. I am confident that you will find creativity in ample abundance in this issue of the *Journal*, as some of the best American and international minds are represented within its pages.

We kick off this discussion with an essay by the oft-quoted, always-opinionated, Mark Lowenthal, whose book *Intelligence: From Secrets to Policy* (4th ed., 2008) has become one of the most widely used textbooks in the various intelligence schoolhouses. Dr. Lowenthal gave a presentation to NDIC students last winter on the subject of intelligence transformation, and I asked if he would convert his verbal wisdom into an article that could be shared with the broader NMIA community. He did so quite amicably, despite a frenetic schedule of running his own intelligence and security training firm, serving as an adjunct at Washington-area universities, and wearing the part-time hat of Executive Director of the International Association for Intelligence Education (IAFIE). He argues that before an entity can expect to transform successfully it must first know why it is transforming and what it hopes to accomplish. Transforming or reforming for its own sake is fruitless if not thought out clearly in advance, which makes one think back to the age-old aphorism, "If it ain't broke, don't fix it!" Retired Romanian General Sergui Medar follows up from a more international perch, discussing some reforms that have emanated from NATO's involvement in Afghanistan. Dr. Medar is a former national security advisor to his country's President and prior to that headed its defense intelligence establishment, much akin to serving in the U.S. as a hybrid of DIA Director and Under Secretary of Defense for Intelligence.

This issue boasts a handful of articles about the proper definition of intelligence itself and whether there needs to be recognition of some new intelligence disciplines, or "INTs," in light of the traditional distinction among HUMINT, SIGINT, and IMINT (now considered a subset of GEOINT) being a Cold War relic of the previous millennium. Army MAJ Charlie Faint argues for the introduction of EXINT, or "Exploitation Intelligence," as a new discipline. The SOUTHCOM J2, Brig Gen (USAF) Dash Jamieson, is promoting a new concept called PACINT, or "People, Affiliations, and Cultures Intelligence," which worked well for that command in responding to recent crises in Haiti. Following on the initiative last year of AFRICOM providing an article about its efforts in the field of Knowledge Development, seen from the perspective of an interagency player and not just a traditional, uniformed COCOM, and now that of SOUTHCOM, we hope to receive assessments in the future from the other geographic COCOMs about how their intelligence missions have been transformed by growing transnational threats. Speaking of those sorts of asymmetric threats, Dr. Jenn Davis of NDIC provides us with an overview of the current transnational panorama as she teaches it to her students.

Personally, I am not so sure what the IC needs is more INTs. Yet another—DOMEX, or Document and Media Exploitation—was highlighted in an article in the May 25 *ZGram* that was published in the Army Intelligence Center's *Military Intelligence Professional Bulletin*. The article argues that DOMEX, referring to analysis of captured enemy documents, should be recognized as an independent intelligence discipline. Yet, other observers have subsumed DOMEX under HUMINT or even OSINT (Open Source Intelligence), depending on the origin of the documents. Frankly, that is one of the major problems with reform and transformation; participants in the debate often cannot come to agreement over terminology and, hence, never get to the meat of the discussion. They spend too much time arguing about form and process and not enough about substance. This problem is delved into by Lt Col (USAF, Ret) Milton Diaz of DIA, who insists that what is needed is a definitional framework for "intelligence." The term means too many different things to too many different people, both practitioners and consumers. To add some even newer terms to the debate, David Moore and Dr.

Robert Hoffman offer an incisive article summarizing their work in the field of "sensemaking," which spawned a book recently published by Moore. He has promised this editor more manuscripts in the future as his team continues to research the concept, which Moore sees as further maturation of critical thinking, the subject of his 2006 work, *Critical Thinking and Intelligence Analysis*.

There are a few carryover articles from past issue themes. Neil Beck weighs in on our earlier "Intelligence and the Rule of Law" theme with his examination of espionage and the law of war. Following up our last issue on "Cyber Security and Operations," DIA's John Schwitz looks at risk-based cyber policy and Dr. Christian Hirst, an Australian expert assisted by his co-author and previous *AIJ* contributor, "Pete" Peterson of NCIS, assesses the cyber threat from the viewpoint of a new tradecraft paradigm. The word "paradigm" comes up frequently in any discussion about transformation; perhaps the idea of a "new paradigm" has become almost trite. We shall let the reader determine that. Even one of the book reviews in this issue adheres to the theme of transformation, which is an assessment of Dr. Bill Lahneman's book calling for a "revolution in intelligence affairs." Dr. Jim Lightfoot assesses whether Lahneman is indeed asking for a full-blown revolution or merely evolution, which seems to be the way the IC has mended itself in the past despite all the breast-beating represented in special commission reports.

This issue is so chock-full of diverse offerings that I will not attempt to mention them all in this brief introduction. However, I do want to draw the reader's attention to some superb articles about current hotspots around the world. Anita Rai, a counterterrorism scholar from the UK, wrote her piece about Pakistan before the latest dust-up created by U.S. unilateral action in taking out Osama bin Laden without prior consultation with the Pakistanis, which makes her observations even more timely now. Garett Tippin looks at democratic development in Afghanistan as an individual with multiple deployments there and to Iraq. A personal story about leadership challenges in being deployed to Afghanistan is provided by MAJ Joe Kosek in the "In My View" section. Dr. Ken Campbell offers yet another glimpse into the life of a past intelligence hero (or villain, depending on where you sit) in our "Profiles in Intelligence" series. This time Ken assesses the long career of East German spymaster Markus Wolf, who remained convinced of the rightness of his and his conflicted nation's political cause to the end.

Looking forward to future themes, to include "Information Warfare" in 2012, and blending it with the present one on transformation, Tom Ranieri examines the need for adapting military intelligence to what he calls "network warfare." Other diverse topics are tackled by, Dr. James McGinley and his fellow Marine intelligence colleagues, who explore motivation in the workplace through a generational prism, and college provost Dr. Andy Sheppard, who offers a fascinating critique of how religion and theology are often overlooked as critical tools in the fight against radical terrorists.

Finally, one of our own dedicated NMIA Board members, COL (Ret) Mike Ferguson, astutely weaves together heartwarming comments from a number of "old hands" who worked with and revered Tom Dillon, long-time HUMINT practitioner extraordinaire for both the Army and DIA. Tom's untimely passing was announced by President Joe Keefe in his column heading up the last issue. Although I saved the piece memorializing Tom for the last few pages of our feature article section, I encourage everyone to read it first. You won't be disappointed; it's truly an inspirational story about an incredible life well lived.

Next fall's issue of the *Journal* will focus on "Counterintelligence, Operations Security, and Information Assurance." I already have some excellent manuscripts in the pipeline but we are always looking for more. I urge you CI professionals out there to share your expertise with our readers; cutoff for initial draft manuscripts is end of October. Articles on other topics are welcome too. The theme for the first issue of *AIJ* in 2012 will be "Cultural Intelligence and Regional Issues." In communicating with this editor in the future, until I know exactly where I will land next after my current contract with DIA expires at the end of July, please write me at spracherw@yahoo.com, or leave a message on my home phone at (703) 646-5931. Cheers to all for a great summer!

Bill Spracher

Transforming Intelligence:
From What, to What?

by Dr. Mark M. Lowenthal

"Would you tell me, please, which way I ought to go from here?"[said Alice].
"That depends a good deal on where you want to get to," said the Cat.
"I don't much care where—-," said Alice.
"Then it doesn't matter which way you go," said the Cat.
"—so long as I get somewhere*," Alice added as an explanation.*
"Oh, you're sure to do that," said the Cat, "if you only walk enough."

— Lewis Carroll, *Alice in Wonderland*

If Jane Austen had been an intelligence analyst she might have begun *Pride and Prejudice* (a title apt for intelligence analysis): "It is a truth universally acknowledged, that an intelligence analyst in possession of a good idea, must be in want of a better means of doing his work."[1]

Many professions see themselves as overly prone to self-flagellation (with the possible exception of lawyers and bankers), but intelligence analysis has to be in the uppermost rungs of the ladder in this regard. Why? I think there are several reasons:

- We recognize the imperfection of what we do. Even though we say that we are not here simply to make calls on future events, that is what much of our work comes down to and we recognize just how difficult this is.
- We deeply love what we do; we see ourselves as a profession (not everyone would agree) and therefore we want to do better.
- Finally, despite the fact that much of what we do is intellectual in nature, we work in a milieu that is strikingly anti-intellectual.

THE ADVENT OF THE DNI: THE BEGINNING OF TRANSFORMATION

The history of intelligence transformation is relatively brief. We may date it from the advent of the Director of National Intelligence (DNI). Ambassador John Negroponte became the first DNI in April 2005. The act creating the DNI, the Intelligence Reform and Terrorism Prevention Act (IRTPA), is worth looking at in this regard. The act that established the U.S. Intelligence Community, the National Security Act of July 1947, was a barebones affair. It said little about the structure and role of the Intelligence Community and contained huge loopholes such as "perform such other functions and duties related to intelligence affecting the national security as the President or the national security may direct."[2] We know, of course, that this referred to operations, but the original act is striking for how little it said about analysis other than the correlation responsibilities of the CIA under the then-Director of Central Intelligence (DCI).

The IRTPA, on the other hand, goes on at great length and in great detail about analysis. It talks about the goals of information sharing, mandates a report on creating an "alternative analysis" function, and requires the identification of some individual who will be responsible for analytic objectivity. Interestingly, at its very outset, the IRTPA talks about the "Transformation of the CIA." Something had clearly happened between 1947 and 2004. Actually, we need not be coy. What had happened had occurred closer to the IRTPA, in 2001 and 2002: 9/11 and Iraq WMD. We tend to see 9/11 as the main driver of the IRTPA, coming as it did on the heels of the 9/11 Commission Report (more formally, the National Commission of Terrorist Attacks Upon the United States), one of the most archly political commission reports ever published. But the various requirements levied on intelligence analysis had very little to do with the findings (let alone the recommendations) of the 9/11 Report; they had everything to do with Iraq WMD and the National Intelligence Estimate (NIE) of October 2002. I have written elsewhere about the various erroneous legends that have grown up around the Iraq WMD NIE and will not

repeat these here.[3] There was clearly a view prevalent in the Congress that flaws in analysis could be fixed through legislation—as if the few points upon which they touched would, of necessity, result in analysis that was less flawed and therefore more likely correct.

The bulk of the Iraq WMD NIE was wrong—although not all of it—and there was a "never again" feeling about intelligence analysis prevalent in Congress and the press. It is also important to recall that in the summer of 2004 the Bush administration, which had been very supportive of the Intelligence Community up until then, had "fallen out of love" and believed, as did *The Wall Street Journal*, that the Intelligence Community was actively working to secure the election of Democratic nominee Senator John Kerry. The result was that the Intelligence Community had no political "top cover" as the IRTPA went through a greatly abbreviated legislative process.

The transformation theme began early under the new DNI. In October 2005, seven months into the job, Negroponte issued his *National Intelligence Strategy*, subtitled "Transformation through Integration and Innovation."[4] One of the mission objectives of the strategy (p. 3) was "[to] Transform our capabilities in order to stay ahead of evolving threats to the United States, exploiting risk while recognizing the impossibility of eliminating it." Later (p. 4), the strategy said, "Transformation of the Intelligence Community will be driven by the doctrinal principle of integration. Our transformation will be centered on a high-performing intelligence workforce that is:

- Results focused
- Collaborative
- Bold
- Future-oriented
- Self-evaluating
- Innovative."

Finally (p. 5), there was a list of ten Enterprise Objectives that would "transform our capabilities faster than threats emerge." There is little to argue about in the actual objectives but it is also difficult to see how they are "transformative." Many of them reflect longstanding and perhaps intractable issues.

BACK TO DEFINITIONS

Part of the problem may be definitional. What does "transform" mean? According to Merriam-Webster, "transform" means "(a) to change in composition or structure; (b) to change the outward form or appearance of; (c) to change in character or condition." One is struck, initially, at how inapt "transform" is when applied to what people have talked about with regard to the Intelligence Community. A secondary reaction is that most people are probably talking about some form of the (c) definition "to change character or condition." But what we have gotten has been mostly (a) and (b), changing composition, structure, or the outward form of appearance.

But this leads to a more important question: How much of what the Intelligence Community does is truly susceptible to transformative change? I would argue that the answer is "Not much."

As much as we all deride the intelligence process (which some erroneously call the "intelligence cycle," even though it is far from cyclical), the process is both sensible and it works.

As much as we all deride the intelligence process (which some erroneously call the "intelligence cycle," even though it is far from cyclical), the process is both sensible and it works. The main steps are and have been:

- Requirements: what do policymakers need to know?
- Collection: what intelligence must we gather to meet the requirement?
- Processing and Exploitation: transforming the collected intelligence into something that can be used by analysts.
- Analysis: what does it all mean?
- Dissemination: choosing the appropriate intelligence product or vehicle to get the right amount of intelligence to the various policymakers who need it, when they need it.
- Consumption: the policymaker taking in the intelligence.
- Feedback: that rare moment when policymakers tell you what they thought of what you gave them—for good or for ill.

One can certainly create any number of ways to define and prioritize requirements. The current system, the National Intelligence Priorities Framework (NIPF), was promulgated under President George W. Bush in 2003 and, quite surprisingly, survived into the Obama administration. The NIPF is not the only system imaginable, although it seems to have a certain durability at this point.

Collection is a question of access. We are always thinking of new ways to give us access to the secrets we need, just as our adversaries constantly seek new ways either to deny us that access or to deceive us. There have been technological breakthroughs that have been "transformative," such as imagery from space-based platforms, but it is highly likely that this is not what most people have meant when they talk about transformation. Processing and exploitation are technical means to plow through as much collected intelligence as possible. Again, breakthroughs have come and likely will come again, but these are not transformative.

This brings us to analysis, which is the central part of the process: creating intelligence products to put before policymakers. Can it be transformed? The problem here is in the nature of analysis. Analysis is an intellectual process – it is about (one hopes) knowledgeable people thinking through problems, coming up with plausible explanations, and writing it up clearly – both in the expository sense and in terms of any nuances, gaps, uncertainties, etc., that need to be emphasized.

Here, again, we have room to make some improvements. The Intelligence Community and many contractors who support them spend a great deal of time looking at new analytic methodologies to see if they are of use. This can, unfortunately, turn into an "ice cream parlor" exercise, as everyone gravitates to the tool that is the new "flavor of the month," whether or not it is applicable to their problem. And here also, we must note, the Intelligence Community still has not come up with a systematic means of testing tools with the people who matter—the analysts—and not the tool makers who invented the tools.

Analysts can be taught different ways to think about problems, about analytical traps, about dangerous mindsets. Indeed, this is necessary, but not transformative. Finally, analysts can and should be taught how to write—as so many analytical managers decry the steady decline of writing skills among people who have finished their college education. But these are all necessary skills, not transformative approaches.

ANALYTIC TRANSFORMATION

In September 2008, then-Deputy DNI for Analysis Thomas Fingar issued his paper, "Analytic Transformation: Unleashing the Potential of a Community of Analysts."[5] The paper listed twelve different initiatives, at least two of which—the NIPF and the Analytic Resources Catalog (ARC)—dated to pre-DNI days, having been put in place during the tenure of DCI George Tenet. There is no value to giving a detailed analysis and critique of each initiative, but it is worthwhile to see what areas they emphasized to get a better view of what the ODNI meant by analytic transformation.

Even before the DNI was created, the Intelligence Community was emphasizing collaboration—but it seemed to mean the antithesis of competitive analysis.

At the outset the report says the goal is to move toward greater collaboration, a word that had become chic in the Intelligence Community in the 1990s, another "flavor of the month," if you will. Many people had different definitions – information sharing, working in teams, etc. But there was also a sub-text here, to use a good analytic term. One of the guiding principles of U.S. intelligence analysis has been competitive analysis: different analysts in different agencies, with different backgrounds and skills all working on the same issue. The assumption was that in such an effort important differences as well as areas of agreement would come out and the subsequent analysis would not be "single-threaded" and would be more likely to come to accurate judgments. Competitive analysis obviously requires a fairly large analytic cadre if we are going to have many analysts across the Community all working on the same issues. But in the 1990s, the intelligence budget cratered as the Intelligence Community—and not the Defense Department—paid for the long awaited post-Cold War peace dividend. The net result was a severe loss of funds and positions. Tenet often said that the Intelligence Community lost the equivalent of 23,000 positions in the 1990s. Thus, competitive analysis became more difficult and was reserved for those highest-value issues, assuming there were sufficient analysts left to do it on a competitive basis. Elsewhere, the emphasis was now on "collaboration" – let's all share because there are fewer of us. It was intellectual triage. So, even before the DNI was created, the Intelligence Community was emphasizing collaboration—but it seemed to mean the antithesis of competitive analysis.[6]

By the time Fingar published his report, the Intelligence Community was awash in new analysts, and operators. The net result now was a decrease in overall expertise. As Fingar noted at the time, over half of the analysts across the Intelligence Community had less than three years experience.[7]

The twelve initiatives grouped into three areas: (1) more integrated analytic operations, which emphasized better means of sharing intelligence and finished work, as well as the now popular communities of interest; (2) better analytic management at the Community level, which included the

Tenet-era NIPF and the ARC, as well as a series of cross-agency activities; and (3) efforts to enhance the quality of analysis, including better tradecraft training, more analytic tools, greater outreach beyond the Community, and the promulgation of analytic standards. Again, few would argue with the goals of these three areas, but were they transformative? I think not – not because Fingar had made an error, but because the real issues did not call for transformation.

One of the issues that did reveal itself as Fingar unveiled his plans was a generational rift. The new analysts were overwhelmingly positive about the proposed innovations. Many of the older analysts, myself included, were skeptical. At a conference in Chicago in September 2007, this generational rift came out in public. Michael Wertheimer, who was then the Assistant DDNI for Analytic Transformation and Technology, laid out the case for transformation and explained how the various initiatives supported this goal. Toward the end of the conference, I asked the same questions I have posed here: what are we transforming, for what reasons, and how will we know if and when we have succeeded? Wertheimer, a superb intelligence officer, admitted that most of the results to date were anecdotal.[8]

My goal here is not to get the last word in this debate. Indeed, Tom Fingar, Mike Wertheimer, and I had many exchanges in the aftermath of the Chicago meeting and found that we had common ground on several goals, such as the need to provide better training for analysts, and to do so on a Community-wide basis. But the overall interest in "transformation" continues to hang like a chimera over the Intelligence Community.

WHERE ARE WE NOW, AND WHERE ARE WE GOING?

We are now two DNIs past the Analytic Transformation paper, in only three years, and some of these initiatives have fallen by the wayside, the inevitable fate of many government programs and ideas.

Despite the passage of time, we remain stuck emotionally and intellectually on the events of 9/11, the Iraq WMD estimate, and their legacy. There remains this strong belief that flaws in the overall analytic process are real, discoverable, and can be remedied either by executive fiat or by legislation. There is also an underlying belief that, with the right tools and the right intelligence and the right working methods, everything that we want to know can be known and that every attempted terrorist attack can be thwarted or disrupted long before it gets to the United States. These views were in evidence as recently as August 2009, during the confirmation hearings for Lieutenant General James Clapper (USAF, Ret) to be the fourth DNI. In an exchange with one of the members, General Clapper sought to disabuse the committee of the notion that intelligence could be right all of the time.[9] Still, the goal – or, rather, the wish – persists.

One of the more recent manifestations of this type of thinking can be seen in a report issued by the National Research Council (NRC).[10] This study was sponsored by the ODNI to see if there was "evidence" from the behavioral and social sciences "relevant to analytic methods and their potential application for the U.S. intelligence community." As could be expected, these two groups of scholars answered in the affirmative. Although the study group evidently reached out to many Intelligence Community veterans, and included one highly regarded former analyst/senior analytical manager among its members, the conclusions and recommendations still seemed odd to many intelligence analysts who read them.[11] Not surprisingly, the first recommendation is for the DNI to apply the "principles, evidentiary standards, and findings" of behavioral and social sciences to virtually all aspects of intelligence analysis. In other words, if you were more like us, it would go better. Second, the DNI should adopt "scientifically validated analytical methods and subject all methods to performance evaluation." Moreover, "Analyses *must* [emphasis added] include quantitative judgments of the probability and uncertainty of the events they forecast." Evidence-based methods should also be used for workforce recruitment and training. Collaboration should be subjected to "systematic empirical evaluations." Scientific, evidence-based protocols should be used to ensure that "analysts and customers understand one another."

We rarely have evidence, i.e., intelligence that is so irrefutable that it can lead to only one conclusion.

Should one weep, shout, or sigh? First, most of this has all been said before. Some of it has even been tried and found wanting. But the most glaring problem is the woeful misunderstanding of what it is that the Intelligence Community does.

- We rarely have evidence, i.e., intelligence that is so irrefutable that it can lead to only one conclusion.
- The amount of methodology in intelligence analysis that is provable is open to question. Very little in intelligence "closes," that is, comes to a conclusion. Intelligence analysis deals mostly with open-ended issues that may change

and alter but rarely conclude. The Soviet Union ends but then the future of Russia becomes an issue. Therefore, it becomes difficult to judge the efficacy of any given methodology as the issue remains open. You probably can make some judgments about different methodologies but these will be based on more limited and therefore more questionable examples.

- The issue of putting quantitative or probability judgments in intelligence analysis is an old one. Those of us who oppose the concept cite the following arguments:
  - First, it suggests a rigor and a precision that is probably false. Why is some event 70 percent certain as opposed to 65 percent? Or 72 percent? How does one make a firm call? It might be possible to create ranges, which would be better, but even these are arbitrary. For example, during the heyday of strategic arms control in the 1970s and 1980s, the Intelligence Community had ranges of confidence regarding its ability to monitor various treaty provisions. The original set was rather stark: High (90-100 percent); Moderate (50-90 percent); and Low (less than 50 percent). But the Carter administration did not like this hierarchy because the SALT II treaty that it was negotiating had too many provisions that fell into the Moderate or Low category. So, they ordered a revision of the confidence ranges. The result was High (90-100 percent); High Moderate (75-90 percent); Moderate (50-75 percent); Low Moderate (25-50 percent); and Low (less than 25 percent). This manipulation made the monitoring calls more politically palatable. It had no effect on Intelligence Community capabilities. "Lies, damned lies, and statistics," as Mark Twain noted.
  - Second, this approach totally fails to take into account the likely effect on a policymaker. If you tell a policymaker that a judgment has 70 percent certainty, he or she is taking that one to the bank. After all, 70 percent is high. What he or she fails to understand, and what those writing the judgment likely will not convey, is that there is also a 30 percent chance (or just under 1 in 3) that the judgment is wrong.
  - Communicating certainty and uncertainty to policymakers remains difficult. In the aftermath of the Iraq WMD NIE, I asked then-NIO for Strategic Programs Robert Walpole to come up with a way to convey estimative judgments to policymakers. The result was the page *"What We Mean When We Say,"* that appears at the beginning of each NIE. The page takes the reader through the use of estimative language and confidence levels. These remain, admittedly, somewhat vague at points, but I think they are less dangerous than somewhat arbitrarily assigned numerical values. Of course, the key question is: do any policymakers ever read this page, even once?
- On the issue of workforce recruitment, the Intelligence Community has figured out how to match needs against applicants, although this became much more systematic after the creation of the ARC. But the Intelligence Community is at the mercy of whoever applies. If not enough Chinese linguists or bio-chemical engineers apply, there is nothing the Community can do about that. As for training, this is one area where the Intelligence Community can learn a lot from the military, especially from the Army. We can and should do better at making training throughout one's career an integral part of every employee's career plan. But to do that we would have to have (1) a better idea as to what analysts' careers look like over time; (2) a more systematic way of describing the skills expected at each level; and (3) courses that help analysts acquire and test those skills.

It really does come down to one desideratum: intelligence that is more accurate more often.

Consequently, we seem to be where we started, struggling to determine what it is we are transforming for what purpose. It really does come down to one desideratum: intelligence that is more accurate more often. Or, put another way, no more 9/11's and no more Iraq WMD NIEs. Taken in reverse order, we can be assured that there will be no more flawed analyses like the Iraq WMD NIE. Instead, there will be other ones, different ones, on different issues that will be flawed for different reasons. Will there be

another 9/11? That is not knowable, but most intelligence officers concede that at some point there is likely to be a successful attack of some sort, perhaps on a lesser scale but still successful. We seem to have lost sight of the fact that this is a war, that the enemy has a will of his own, and that he will try to operate on our soil. We cannot dictate the theater of engagement any more than we can expect perfection in discovering every planned attempt.

There are several things that we can easily accomplish that would, I believe, have a transformative effect on intelligence analysis:

- As I have written elsewhere,[12] having a serious conversation among intelligence professionals, their policy customers, Congress, and even the press on what can reasonably be expected of intelligence, both overall and against specific issues, would be extremely useful. A set of probably general standards but shared expectations would be transformative for intelligence and extremely liberating. Instead of worrying about each new round of "gotcha," analysts might be willing to take risks, to push their analyses further, knowing that omniscience and perfection were not the standards.
- Getting back to basics. We have to get back to the "knowledge building" business. We were very good at this during the Cold War but seem to have lost the capacity. Too much of what we do is esoteric. This was one of the basic critiques of Major General Michael Flynn's January 2010 paper, "Fixing Intel."[13]
- It is true not only about Afghanistan but across the board in intelligence analysis.
- Closely tied to the previous point, putting more emphasis on expertise and depth among analysts. This runs counter to how many of the new analysts hope to manage their careers but we need experts, not analysts who flit from subject to subject.
- Recognizing that many of the new analysts lack the writing and organizational skills (preparing an outline) that we once took for granted. As frustrating as it may seem, we need to spend more time on these skills with the analysts at the very outset of their careers.
- Training the way we fight, as the military puts it. If we want analysts to work collaboratively across the Intelligence Community, then we have to train them in Community-wide courses, again from the outset of their careers.

- Getting the National Intelligence University (NIU) up and running as the center of Community-wide education and training, creating standards and course requirements, and thinking about what analysts' careers look like and what sort of training they will need across their careers.

"[Get] the National Intelligence University (NIU) up and running as the center of Community-wide education and training."

It is less about analytic tools and nifty new technologies, or gratuitous advice from people who have no appreciation of what we do. Getting back to basics in a serious, Community-wide way would be truly transformative.

Notes

[1] Apologies to Jane Austen, *Pride and Prejudice*,1813.
[2] Sec. 104A(d)(4) of the National Security Act (50 USC 403-4a).
[3] Mark M. Lowenthal, "The Real Intelligence Failure? Spineless Spies," *The Washington Post*, May 25, 2008. Available at <http://www.washingtonpost.com/wp-dyn/content/article/2008/05/22/AR2008052202961.html>.
[4] *The National Intelligence Strategy of the United States of America*, October 2005. Available at <http://dni.gov/publications/NISOctober2005.pdf>.
[5] This paper is available at <http://www.dni.gov/content/AT_Digital%2020080923.pdf>.
[6] When I became the Assistant DCI for Analysis and Production in 2002, I found that my new staff included a collaborative analysis group whose viewpoint was exactly as described above—the antithesis of competitive analysis, sharing for sharing's sake. I disbanded the office immediately and moved all of the officers to other, more useful, assignments, where they flourished.
[7] Conversations with Thomas Fingar, 2008. As of April 2011, the figure is that half of the analysts have less than five years of experience—better, but still alarming.
[8] Wertheimer's explanation of analytic transformation, as well as the exchange between us, can be found in Shane Harris, "Intelligence veteran aims to motivate young analysts," *National Journal*, September 24, 2007, at <http://www.govexec.com/dailyfed/0907/092407nj1.htm>.
[9] Conversation with one of the hearing participants, April 9, 2011.
[10] "Intelligence Analysis for Tomorrow," The National Research Council, Washington, DC, 2011.
[11] My evidence here is clearly anecdotal but uniform among many of my colleagues with decades of intelligence analysis experience.
[12] Mark M. Lowenthal, "Toward a Reasonable Standard for Analysis: How Right, How Often on Which Issues?" *Intelligence and National Security*, Vol. 23, No. 2, June 2008, 303-315.
[13] Major General Michael T. Flynn, Captain Matt Pottinger, and Paul D. Batchelor. "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Center for a New American Security, January 2010. Available at <http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf>.

Mark M. Lowenthal is President and CEO of the Intelligence & Security Academy. He has served as ADCI for Analysis and Production and Vice Chairman for Evaluation on the National Intelligence Council. He was staff director of the HPSCI in the 104th Congress (1995-97) and directed the committee's study on the future of the IC, IC21: The Intelligence Community in the 21st Century. *He served in the State Department's Bureau of Intelligence and Research as both an office director and a Deputy Assistant Secretary of State. He was the Senior Specialist in U.S. Foreign Policy at the Congressional Research Service/Library of Congress. Dr. Lowenthal has written extensively on intelligence and national security issues. His most recent book,* Intelligence: From Secrets to Policy *(Sage/CQ Press, 4th ed., 2009), has become the standard college and graduate school textbook on the subject. The author received his BA degree from Brooklyn College and his PhD in history from Harvard University. He is an Adjunct Professor at Johns Hopkins University and he was an adjunct at Columbia University from 1993 to 2007. In 2005 he was awarded the National Intelligence Distinguished Service Medal. In 1988 he was the Grand Champion on the television quiz show* Jeopardy!

Military Intelligence Transformation:
Accomplishing New Missions in Response to the Recent NATO Strategic Concept

by General (Ret) Sergui Medar, Romania

It is a well-known fact that intelligence transformation is a continuing process. This is because of the dynamic nature of the world's transformation and, accordingly, the evolution of world threats is a rapid and continuing process. Intelligence must not only keep pace with the evolution of threats but stay one step ahead and forecast them. This means that intelligence organizations must continuously update their structures, procedures, doctrines, and ways and means to act. There is not enough time to wait for stabilizing the current structures or for a long process of building trust leading to cooperation. To be successful, it is always necessary to take a calculated risk; decisions must be quick and soundly justified. This is well known as a proactive behavior, not a reactive one. Pessimism and suspicion always delay the process and the result is obvious—failure. Sometimes the "bad guys" are more dynamic and creative than us, but we will be one step ahead of them if we cooperate, train together, and trust each other.

The new NATO Strategic Concept took into consideration the emerging world threats, defining new missions in accordance with it. At the same time, this concept used NATO lessons learned in facing the current threats. Therefore, the inevitable result is new intelligence tasks for our respective countries.

The major change in the NATO Strategic Concept, with an important impact for NATO Intelligence, is mentioned in paragraph 36: *"NATO is a **security Alliance** that fields military forces able to operate together in any environment"* [emphasis added]. This underlines the fact that military intelligence continues to be one of the core intelligence operational providers, but extending the definition of the Alliance to being a "security Alliance," with many of the intelligence tasks belonging to other types of intelligence services (internal and external civilian intelligence services). In a multinational environment, cooperation among all these services is the only way to drive the Alliance toward success.

This transformation from a politico-military Alliance into a security Alliance was not an unexpected one. The Riga NATO Summit Final Declaration mentioned, for the first time, security of the energy transportation infrastructure as a NATO mission. Military capabilities were not the first option for action, but intelligence capabilities have been considered in the first line of defense. These are not primary tasks for military intelligence, whose main missions are not initially directed toward the security of energy resources and the transportation infrastructure. All the discussions surrounding non-military issues underlined the fact that the solution for this new type of NATO mission, alongside the fight against terrorism, revealed the necessity for cooperation among non-military intelligence services within NATO intelligence communities. Participation of these services in the context of the fusion intelligence concept and, even more so, the NATO Fusion Center is now a key factor.

This transformation from a politico-military Alliance into a security Alliance was not an unexpected one.

The new NATO Strategic Concept, in terms of Crisis Management being a core NATO task, mentions: *"NATO will actively employ an appropriate mix of those political and military tools to help manage developing crises that have the potential to affect Alliance security, before they escalate into conflicts; to stop ongoing conflicts where they affect Alliance security; and to help consolidate stability in post-conflict situations where that contributes to Euro-Atlantic security."*

Paragraph 20 from the same document underlines the fact that *"NATO will therefore engage, where possible and when necessary, to **prevent** crises, **manage** crises, **stabilize** post-conflict situations and **support reconstruction**"* [emphasis added].

This concept presumes military operations in a variety of complex pre- and post-conflict environments. For achieving this mission, the military planners have to include elements of economic, social, and political, as well as military, power. The future strategic military plans will

necessarily assume a kind of hybrid approach, bringing together a spectrum of elements of national institutions. Up to now, projection of the diplomatic, administrative, educational, internal security, informational, and economic components of national power, plus development of the programs to rebuild and to enhance new states, has been under the jurisdiction of interagency, non-governmental, and international organizations. Following the lessons learned of previous and current NATO missions, it was clear the militaries always did their job, won the wars, but even more or less peace was brought to former areas of operations, the new states. For a long period of time, however, these states were not able to manage their own fate by themselves. Now, in accordance with this new concept, NATO, using its capabilities, will assume the burden of coordinating the building process of the new environment, including new states.

Nevertheless, where a hostile environment precludes deployment of civilians to implement such missions, NATO will become the only viable organization for succeeding in this task. For many of the NATO countries this is a new mission but not for the United States, which in the last few years has been deeply involved in this kind of operation.

According to many analysts, future wars will be "hybrid wars."

According to many analysts, future wars will be "hybrid wars." Besides the effort in obtaining the support of the local population and the international community, another main characteristic of these wars is projecting all elements of national power along a continuum of activities from stability, security, and reconstruction operations to armed combat. At the same time, these are conflicts in which armed forces must be able to face high- and low-intensity warfare, sometimes in the same period of time.

Seen by some military analysts as controversial, the "hybrid war" concept tries to underline the new approach of using armed forces for preventive measures, as components of preventive and coercive diplomacy, in very well-known "operations other than war," combat operations, and post-conflict stabilization and reconstruction efforts. This last mission can be seen as a process of capitalizing on all the achievements gained from previous participating phases.

Hybrid wars bring into discussion hybrid threats, which take into consideration countries' vulnerabilities before and after the conflict. These two types of vulnerabilities are very different in nature, as is the way to address them and the environment in which to act. This requires employment of a wide and comprehensive variety of military and non-military activities, programs, resources, and procedures capable of acting as well in the economic and political environment and against criminal activities such as smuggling; narcoterrorism; illicit transfers of advanced technologies, ammunition, and weapons; actions of urban gang networks; and, last but not least, terrorism.

All these non-military activities must be performed or coordinated by the militaries. The final goal is to avoid destabilization of a state where usually the economy is in deterioration and the state of law practically no longer exists. These actions require a full range of intelligence capabilities; public and defense diplomacy tools; use of unconventional, sometimes non-lethal, armaments; and other ways and means at the limits of combat action but capable of switching to a combat operation immediately when the opposition elements of regular forces or irregular insurgents, terrorists, or other non-state actors cross the hostility threshold and constitute a direct threat to these non-hostile activities.

The new NATO military and non-military activities should be included totally or partially in this category of hybrid warfare. This kind of activity requires a full spectrum of intelligence approaches specific to all kinds of intelligence organizations. Are NATO intelligence structures prepared for preventing conflict and monitoring the conditions and the background for future conflict, present conflict, and post-conflict intelligence operations?

The needed activities for crisis prevention are comprised of: fighting against corruption and organized crime, recommending and implementing measures to stop economic recession, enhancing law enforcement and border control capabilities, cooperating in counterterrorism activities, discouraging urban gang activities, organizing media stabilizing activities, promoting humanitarian aid distribution and health support, and enhancing public safety and other stabilizing activities.

Intelligence for the prevention of conflicts is mostly the domain of foreign intelligence service capabilities. They can cooperate with the military intelligence services, which usually have limited capabilities for this stage. NATO should work with foreign intelligence services as a prime contributor of specific intelligence for conflict prevention solutions.

Military intelligence is always prepared, trained, and has legal and operational capabilities for evaluating the risks and threats in an area before a crisis, for the so-called "Phase 0" to acknowledge and shape the future combat environment. This includes the purpose of military preparations for a crisis and providing to the military

decision-making level during the crisis the most appropriate actionable intelligence product.

When the crisis is unavoidable and a future military action is imminent, military intelligence starts to acknowledge and monitor the environment and conditions for a future possible deployment. It also updates the local situation's conditions and coordinates future possible targets, delivering the necessary intelligence for logistical support and other specific military intelligence activities.

This is the moment when cooperation between foreign intelligence and military intelligence is critical. Foreign intelligence must transfer to military intelligence the critical knowledge and capabilities it was able to build into the preventive conflict phase, which will be used by military intelligence in combat intelligence operations.

In combat operations, NATO intelligence relies mostly on production by the military intelligence services. For war and antiterrorist combat intelligence operations there are clear doctrines, regulations, procedures, and ways and means of acting. This is obviously the primary field of military intelligence operations. Foreign intelligence production is still necessary in this phase, filling out the local and regional picture with valuable and updated intelligence products directed to the common goal of NATO force missions in the area of operations.

According to the new NATO Strategic Concept, the Alliance will coordinate, will lead, and will participate in post-conflict operations.

According to the new NATO Strategic Concept, the Alliance will coordinate, will lead, and will participate in post-conflict operations. There are not yet very clear doctrines for post- conflict operations as well as doctrines and procedures for post-conflict intelligence operations. This kind of intelligence operation requires a common approach across the entire spectrum of intelligence services. This necessary intelligence contribution should come from a "consortium" of intelligence services focused on the "target-centric approach," where, at least, the concept of "3FEA" (Find, Fix, Finish, Exploit, and Assess) could be a matter of daily common interest. [Author's note: This is a new concept developed as a "lesson learned" from the conflict in Afghanistan. It is in essence a new version of the intelligence cycle coming from the field but with application to strategic intelligence.]

For the reconstruction process of a country there are many other organizations and institutions necessary besides the military institution. Militaries have to continue to provide the necessary level of security for the rebuilding process. At the same time they must train local military forces to help them manage by themselves and to be able to take the security burden into their own hands. The transfer of these responsibilities is a difficult process which demands a lot of patience.

The post-conflict environment is even more complex than the pre-crisis environment. This is because a real state does not yet exist. The necessary activities are specific for a state rebuilding phase: population census, free local and general elections, reorganizing administrative organizations, reorganizing security institutions, organizing NGOs capable of overseeing the democratic transformation of the country, etc. All of these activities must be performed in a volatile security environment when the reversibility of the democratic process is possible at any time.

Enhancing the capabilities of the new democratic security local institutions is a very tough and demanding process. Cooperation with the new institutions is difficult and requires intense efforts to avoid mistrust or lack of trust, but at the same time to prevent any leaks of intelligence. NATO participation at this phase of post-conflict operations is critical and is a very difficult mission given the participation of various institutions, each of them with a different culture. When this becomes a mix of different institutional cultures and different nationality cultures, the most workable way to succeed is to have precisely agreed to procedures to act.

At this phase a good and accurate actionable intelligence production plan is critical for assuring success. The process of transferring intelligence capabilities among intelligence services is the reverse compared with the first phase mentioned above. Military intelligence should transfer some of its suitable intelligence capabilities, built during combat operations, to the foreign or domestic intelligence services.

Because military intelligence participated in the pre-conflict intelligence collection and analysis phases, and in actual combat intelligence operations, when the post-conflict intelligence operation starts, the players already have a comprehensive database regarding the area of involvement, a deep knowledge of the local situation, and an efficient and trustworthy source network which means an overall and updated common intelligence operating picture. To share this common intelligence operating picture, creating databases and networks with the new post-conflict intelligence operational partners is

not enough. People with experience in the field know very well how difficult it is just to transfer all of this to new partners having a different approach, mentality, and sometimes culture. This is why the only solution is to share capabilities with the new partners. This is very difficult between partners from the same country, but sometimes this "consortium of intelligence services" belongs to different types of services from several different NATO countries.

To assure the necessary security level in a country once the war is over, often needed are counterinsurgency and counterespionage activities. The new state does not yet possess the appropriate capabilities for such kinds of protection missions, the lack of which can easily destabilize the new state. This is why it is preferable for counterinsurgency and counterespionage to be performed for the new state, at least in the beginning, by NATO countries' intelligence services. This is not a primary task for a military intelligence service, but more so of the internal national service in cooperation with foreign intelligence services. This "consortium of intelligence services" of NATO countries is a new challenge for all our services. In some member countries such experience can be found, but only at the national level, not the international.

The key for the last NATO combat intelligence mission's success was the ability to share capabilities, not just intelligence.

For a long period of time "to cooperate" had the meaning of "to share intelligence." Today's missions prove the fact that sharing intelligence in NATO operations is not sufficient. This is why the key for the last NATO combat intelligence mission's success was the ability to *share capabilities*, not just *intelligence*. At the beginning, there was a lot of skepticism and suspicion regarding this process.

The good news stemming from this kind of difficulty is that the experience of some NATO countries in a quite similar kind of cooperation was proven to be possible. The intelligence cooperation necessary to accomplish the new missions according to the NATO Strategic Concept must be performed not only between intelligence services belonging to the same country but among different intelligence services from different countries. This is not easy. It is a matter of culture, training, procedures and, in the end, the most important commodity of all—*trust.*

Exchange of experience, training together, conducting simulations, sharing critical intelligence, and sharing capabilities are only a few ways to build the necessary trust and operational compatibility for common operations in all phases of the peace and stability-building process. Education and training of specialists brought together from the different services of the same country or from different NATO countries, at the initial stages, is one of the keys to future success. This does not mean only to utilize common procedures and common professional language but to share the culture with each other, to build trust and even friendship which, later, will help during real-world mutual operations. This will eliminate the mistrust and suspicions which up to a level are normal; however, all of us must avoid this handicap.

Intelligence operations in missions aligning with the new NATO Strategic Concept are an opportunity for intelligence service cooperation by NATO countries and non-NATO countries alike. Speaking of intelligence cooperation, not only sharing information should be taken into account but also cooperation among NATO and non-NATO countries. This means first identifying the common strategic interests of a NATO and a non-NATO country. They can cooperate when aligning with these common interests—for example, narcoterrorism. For certain, the fight against this threat is a common interest. The two countries can easily cooperate on this target.

The world will gradually become more and more complex. The security approach will prevail compared to the purely military approach. Military tools must be the ultimate solution in achieving peace. When we talk about the security approach, however, this means the importance of defense diplomacy, with both sides' preventive diplomacy, coercive diplomacy, and actionable intelligence production. This signifies a huge responsibility for our intelligence organizations, whose cooperation is key.

General (Retired) Sergui Tudor Medar is the former National Security Advisor to the President of Romania (2005-07), leading the National Security Department and the Operational Committee of the National Intelligence Community. Prior to that critical

assignment, he was Director General for Defense Intelligence (2005), Director of Military Intelligence (1999-2005), and his nation's Assistant Defense Attaché and then Defense Attaché to the U.S. in Washington, DC (1992-99). He currently serves as President and CEO of SM World Solutions, Inc. He is also Professor of Security Studies, Defense Diplomacy, Crisis Management, and Corporate Security Management at Lucian Blaga University in Sibiu, Romania. Gen Medar earned his PhD degree at the Polytechnic University of Bucharest in 1986. He has also received postgraduate certificates from the National Defense University and the Postgraduate Studies Center, both in Bucharest. He is the author or co-author of eight books, numerous articles, and 25 technical research studies. His most recent publications include "Military Intelligence in a Changing World," "Intelligence for Commanders," and "Modern Military Intelligence Capabilities" (all 2007). He holds the Legion of Merit (officer rank) as a result of his attaché service in the U.S. In the fall of 2010, he served as a visiting scholar at the Center for International Engagement, National Defense Intelligence College, in Washington, and was one of the principal founders and organizers of that Center's series of annual Black Sea and Caspian Sea Symposia, the second iteration of which was hosted in May 2007 by Dr. Medar's native country in Constanta, Romania.

People, Affiliations, and Cultures Intelligence (PACINT):
Harnessing the Voice of Populations to Improve Strategic Warning in the 21st Century

by Brigadier General (USAF) Dash Jamieson
and Lieutenant Colonel (USAF) Maurizio Calabrese, U.S. Southern Command

As our case is new, we must think and act anew.

– Abraham Lincoln

INTRODUCTION

Erosion of strategic warning, as a result of the post-Cold War environment, an emphasis on post 9-11 overseas contingency operations (OCO), and an ever-present era of budget efficiencies have established the need for new thought processes to fill intelligence gaps. As observed in recent events throughout the Middle East and North Africa, no traditional intelligence, surveillance, and reconnaissance (ISR) asset provided strategic warning of impending changes that would result in U.S. decision-makers needing to take action. However, any Soldier, Sailor, Airman, Marine, or civilian analyst sitting on the Internet at the right place at the right time could have provided the information needed to generate action.

This emerging information environment requires a paradigm shift among Intelligence Community (IC) leaders to ensure the IC is able to transform itself to recognize the current ISR inventory does not address the reality of the current global construct. No ISR ground sensor, ship, submarine, aircraft, satellite, or human asset is poised to collect what very well may be the empowered 5th generation fighter. However, unlike the thoughts of T.X. Hammes, the 5th generation fighter is not a small group empowered by technology, but it is a collective—a socially connected, mass network of individuals empowered not by weapons, but by ideas to either create or to change the status quo of a nation-state.[1] Unlike Al-Qaida or other terrorist movements which attract the fringes of society, this new 5th generation fighter is society itself. The mass distribution of the Internet, cell phones, and wireless technology across the globe has finally given "the people" a voice.

The Clausewitzian trinity of war consisting of blind natural force, probability, and the instrument of policy (aspects illustrated by the people, military, and government respectively) has finally come to fruition. The IC, for the first time, can now tap into not only the intent and capabilities of adversary governments and military forces, but into the voice of the people themselves.[2] Classic indications & warning has never focused on the people as an actor in their own right, but today's Information Age demands it.

The U.S. National Security Strategy states the U.S. government's primary mission is to defend the homeland through all instruments of power. A need for worldwide engagement, awareness, and action is fundamental to being a responsible global leader. Successful employment of this strategy requires the U.S. government to rely on strategic indications & warning (I&W) to provide decision-makers valuable context and characterization in order to shift emphasis in established priorities and consider actions through the diplomatic, information, military, and economic (DIME) instruments of power construct. Strategic warning sets the conditions for decision-makers to prudently use the appropriate DIME resources to respond to crises without needing to focus solely on a military response. This article puts forth the idea of creating a new intelligence discipline known as People, Affiliations, and Cultures Intelligence (PACINT) to address the indicators decision-makers need for situational awareness and establish critical components of a new strategic warning methodology for the 21st century.

STRATEGIC WARNING INTELLIGENCE EROSION

There are several factors contributing to the erosion of U.S. strategic warning capabilities. First, there was the collapse of the Soviet Union, which left North Korea as the prime remaining "Cold War" issue with a classic I&W problem. Second, there is an increasing lack of regional access of ISR sensors to acquire strategic intelligence information across the globe due to national

priorities, declining resources, fiscal constraints, and increased anti-access technologies denying traditional sensors the ability to collect information. Third, there is the lack of experience among the OCO generation of analysts on what strategic warning really means. Analysts who have entered the IC since 9/11 have learned strategic warning concepts in the context of preventing violent extremist organization attacks against the homeland. This narrowed focus is not a criticism, as the lack of any attacks since 9/11 within the United States has proven intelligence analysts are more adept at strategic warning against the irregular adversary. However, even within an irregular warfare environment, MG Michael Flynn, Capt Matt Pottinger, and Paul D. Batchelor highlighted how senior leaders are still failing to receive timely information from the tactical level that might have strategic-level importance. Analysts are "starved" for information from the ground level, and they need to have "population-centric information as the lifeblood of their analytical work."[3]

In a similar fashion, senior leaders at the Combatant Command level need to be apprised of tactical-level activities within their areas of responsibility (AOR) that may have strategic implications. The recent events in Tunisia, Egypt, and Libya are all examples of how tactical activities had strategic-level outcomes, the latter of which directly involved U.N. sanctions, economic restrictions, and the commitment of U.S. and coalition combat forces. Yet, none of the aforementioned events was predicted or even anticipated because of a lack of strategic warning. Hindsight has proven (as it always does) that indicators were available, especially via open- source products covering foreign and social media. However, there is no specific single intelligence discipline addressing how to leverage these types of sources on a mass scale to take advantage of crowd-sourcing and to understand tipping points along the social landscape. Increased global connectivity and the speed with which information flows via social media sources means it is time to shed the 20th century Cold War paradigm of relying exclusively on traditional "INTs" and develop a new paradigm to advance thought on strategic warning for the 21st century. PACINT provides a way forward to take advantage of technological changes and increased global socio-cultural knowledge to ensure the IC remains adaptable and relevant by harnessing population-centric intelligence as part of a new strategic warning methodology.

A BRIEF HISTORY OF INTELLIGENCE DISCIPLINE DEVELOPMENT

The earliest known intelligence discipline is human intelligence (HUMINT). Though not defined as such, the use of humans to conduct surveillance against adversaries is recorded throughout ancient history. However, it was in the late 19th and throughout the 20th century when an explosion of technologies created new intelligence disciplines. The invention of the photograph provided an ability to capture images over a battlefield or area of interest from the high ground, whether a hill, a balloon, an aircraft, or a satellite. This imagery intelligence (IMINT) later transformed into geospatial intelligence (GEOINT) when technological tools became more readily available to allow traditional "mapping" and "imagery" products to be combined into multi-dimensional, multi-layered visualization products for situational awareness. Signals Intelligence (SIGINT) began with the invention of wire and voice communications through the telegraph and the telephone. Yet, SIGINT as a discipline evolved over time as technology advanced. The invention of radars and missile technology created the electronic intelligence (ELINT) and foreign instrumentation signals intelligence (FISINT) sub-disciplines, which combined with traditional communications intelligence (COMINT) to define SIGINT today.

Likewise, Measurement and Signatures Intelligence (MASINT), generated from the understanding of acoustics to determine ranging and classification, has become more diverse over time as it seeks to incorporate other intelligence disciplines to provide specialized information to decision-makers.[4] Open-source intelligence (OSINT) is generally accepted as one of the more recent 20th century foundational INTs. However, its roots began with radio translations as part of the Princeton Listening Center in 1939 and the establishment of the Foreign Broadcast Information Service in 1941.[5] OSINT has adapted over time to make use of print media, academia, and the Internet to provide additional insights into foreign activities.

None of the current disciplines has achieved a persistent capability to capture the exponential growth of social media, socio-cultural awareness, and the ability to provide crowd-sourced intelligence on a global scale.

The shortcoming of all these INTs in the 21st century is that traditional ISR only captures what Clausewitz referred to as the government and the military legs of his famous trinity. None of the current disciplines has achieved a persistent capability to capture the exponential growth of social media, socio-cultural awareness, and the ability to provide crowd-sourced intelligence on a global scale. The "people's voice" can only be addressed in the traditional INTs through anecdotal reporting from SIGINT, HUMINT,

and the majority of OSINT, all of which are subject to the original source's interpretation and distortion. The people, as a crowd, provide uncontrolled, raw, and emotional information that can complete the Clausewitzian trinity. PACINT seeks to capture these data as a key component for a new 21st century strategic warning mindset.

A NEW DISCIPLINE: PEOPLE, AFFILIATIONS, AND CULTURES INTELLIGENCE

Defining a new intelligence discipline is a complex task. Ideally, it should focus on relevant information sources that are available and obtainable. More importantly, a new INT needs to be repeatable, predictable, and verifiable so that personnel can be trained, collection requirements can be levied, and analysts can characterize the source to provide accurate assessments. A new discipline should also be mutually exclusive from existing disciplines as defined by Joint Publication 2-0, *Intelligence*. Exploring the proposed People, Affiliations, and Cultural Intelligence discipline in more detail will highlight how PACINT meets these requirements.

PACINT is defined as the fusion of people-driven, dynamically available social media and socio-cultural-based awareness and analysis coupled with open-source information to generate timely and relevant crowd-sourced intelligence (see Figure 1). Within the PACINT acronym itself, "People" is defined as the body of persons that populate a nation-state. "Affiliations" is defined as the association of people into specific political or socio-cultural identities such as groups, tribes, or classes. "Cultures" are defined as the behaviors and beliefs of a particular affiliation. These three elements, People, Affiliations, and Cultures, are critical to understanding the social landscape and the indicators necessary to conduct all-source strategic warning analysis. Examining PACINT's principles in more detail highlights why PACINT deserves its own recognition as a new intelligence discipline for the 21st century.

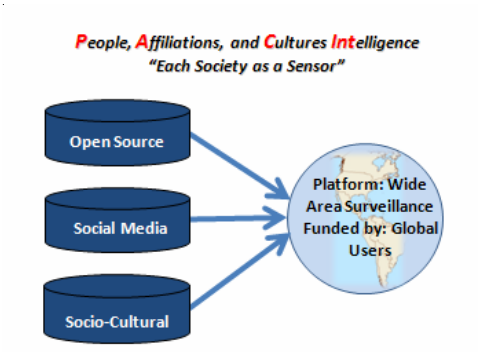


Figure 1. PACINT Fundamentals

The first principle of PACINT is that it is people-driven and dynamically available. While this discipline could be obtained from more classic media such as newspapers, books, pamphlets, radio broadcasts, the expectation in the 21st century is that PACINT also will be collected via social media, blogs, and social network forums. The free flow of information between non-state actors across the globe is best enabled through wireless communications and the Internet, which allows for rapid transfer of ideas. This connectivity is a strong tenet of why PACINT is a viable discipline as part of a new 21st century strategic warning methodology. I&W can no longer be confined to government and military force postures and readiness levels since nation-state populations have emerged as globally-linked non-state actors. The nearly instantaneous spread of thoughts via social media can result in a grassroots mobilization within hours if a relevant social landscape trigger has been pulled, resulting in a tipping point for the population to generate unrest.

The idea of social mobilization is not new, but identifying independent and dependent variables that triggered a movement is typically done in hindsight. PACINT would seek to predict these mobilization events using the dynamic resources available in real time instead of hindsight. The intent is to forecast which "social" messages will trigger not merely a reaction from the population, but a movement so critical that it becomes "viral" and threatens to change the status quo within a nation-state.

The second principle of PACINT is that it is socio-cultural-based. Understanding the political, religious, economic, and social norms affecting global societies is necessary to understanding the social landscape aspect of this new discipline. If one does not understand the history of a nation, nor the issues most important to its people, then PACINT is simply OSINT by another name and cannot become proactive. For example, recent open-source news media coverage of a Florida church burning a *Qur'an* would not necessarily go "viral" within the United States or Latin America because Muslim communities remain a relatively small portion of the population.[6] Therefore analysts at U.S. Northern Command (NORTHCOM) or U.S. Southern Command (SOUTHCOM) would deduce that such coverage is unlikely to have any nation-state effect in their respective AORs and monitor open-source reports for any blowback.

Conversely, an analyst in U.S. Central Command (CENTCOM) would request PACINT coverage for I&W since the same news piece, when spread rapidly through dynamic social media tools (e.g., blogs, Facebook, Twitter), could result in force protection threats to U.S. forces throughout the CENTCOM AOR. Likewise, an analyst at U.S. Pacific Command (PACOM) who sees the same

information may deduce there will be no action despite cultural sensitivities, because PACINT has revealed no heightened "dynamic" activity suggesting any threat. All three of these examples highlight how understanding the social landscape can provide the analytical baseline for predicting a people-driven event. A key difference between OSINT and PACINT, however, is the latter's focus on the population's reaction through social media to proactively understand when and where unrest may occur.

The third principle of PACINT is that it must be crowd-sourced. The goal of PACINT is to identify when and where grassroots movements will take action within foreign countries based on resonating social messages. PACINT is most effective when analysts are researching mediums that give "the people" a voice to share their ideas, concerns, and calls for action. The number of "visits," "posts," or "ratings" for various online or mobile media can provide some indication of the speed at which a message is spreading and how popular it is with the people. There are already tools in existence which can highlight how much "traffic" an Internet site is generating, but that is not sufficient to determine if the people have the *capability* and *intent* to take action. Traditionally, analysts consider a threat to be viable when these two components are linked together. Neither is sufficient in itself to generate a threat warning, but the presence of either capability or intent warrants analysts to provide additional monitoring. A population en masse is assumed to have a capability to protest at a minimum, but PACINT would provide the strategic warning needed on the population's intent.

One model to understand the importance of crowd-sourcing is Everett Rogers' Adoption/Innovation bell curve, essentially defined by three sections: early adopters, mainstream adopters, and laggards.[7] Traditional ideas usually begin with a few supporters who spread the message. If the message appeals for mainstream support grows exponentially through the majority, this would be the equivalent of an issue going "viral." As time moves on, the laggards join the cause, but by then most of the fervor has waned. PACINT uses social media to understand when a message is moving from the early adapters to the mainstream to provide adequate strategic warning (see Figure 2).

Of course, the analyst must have the socio-cultural awareness to understand if the target population has access to readily obtain social media-based information. Assuming the population does have this access, focusing on the "crowd" is what will finally give intelligence analysts insight into the emotional, uncontrolled environment of the people to complete the Clausewitzian trinity.

While the definition of PACINT is mutually exclusive to other intelligence disciplines, these three principles of PACINT are mutually inclusive, as none of them is

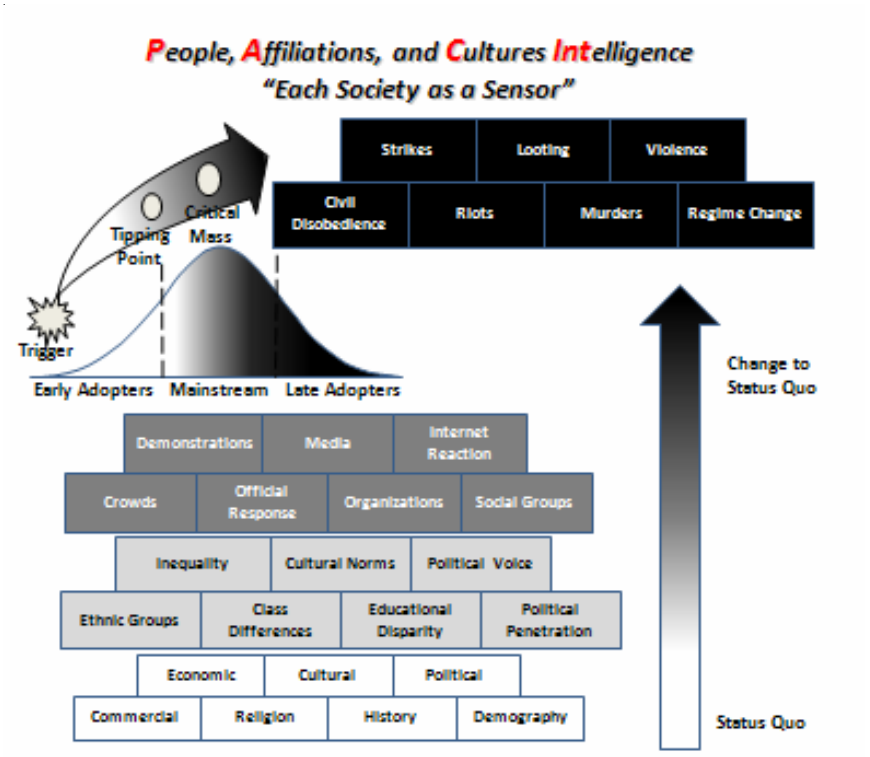


Figure 2. PACINT Social Landscape

sufficient by itself to be considered PACINT. In fact, that is what makes PACINT a separate discipline worthy of inclusion in all-source analysis. If an analyst studies the communications links and nodes within a country, they have perhaps conducted some SIGINT, HUMINT, OSINT, or GEOINT, depending on the source of the information. If an analyst obtains some print media or radio broadcasts, he or she has conducted OSINT on "controlled" sources which are either influenced by or targeted at foreign government actions. If an analyst studies the socio-cultural dynamics of a nation, he or she has obtained baseline knowledge of multiple factors, which is not dissimilar from scholarly regional area studies. These studies cannot be considered intelligence, and again they are usually based on reading information from "controlled" sources (universities, interviews, journal publications, etc.). However, if an analyst reads a blog from someone affected by a government decision, he or she is receiving raw, unevaluated, uncontrolled data without any context. Further analysis is needed to determine whether the message is dynamically available to other readers and whether the conditions are ripe for such a blog to reach a population tipping point and go "viral." PACINT is achieved only when the uncontrolled population perspective has been obtained through dynamically available social media with an underlying understanding of the social landscape.

Forming a new intelligence discipline based on using intelligence derived from other sources has precedent. The most obvious example is the MASINT discipline, which can provide products derived from GEOINT, SIGINT, HUMINT, and other sources. Arguably MASINT is probably the least understood of all the INTs for the precise reason that it does not focus on a single source to provide its information. However, its approach is most similar to PACINT in that it is a specialized field that can provide a unique perspective on a given problem set. An argument could be made that PACINT is a sub-discipline of MASINT, but the socio-cultural aspect of it does add a degree of subjectivity that is not found in MASINT, which traditionally uses "hard science" to provide intelligence.

When examining the other intelligence disciplines, PACINT remains separate and distinct. Since PACINT is based on population-provided information, an argument can be made that it is a sub-discipline of HUMINT. Yet, crowd-based sourcing is what makes PACINT the exact opposite of HUMINT because it cannot task, vet, or provide the reliability of any source. HUMINT seeks to provide "controlled" information where the analyst is given requisite information on source reliability and reporting history to make a determination on the validity of intelligence provided. Additionally, HUMINT sources are based on access to information, and PACINT by its nature means that thousands, if not millions, could have access to the information. As such, HUMINT is not the parent discipline of PACINT. PACINT assumes the "crowd" itself is reliable because the sheer magnitude of perception provided makes this non-state actor's self-perceived reality into the new reality for the nation-state government or military.

Given that PACINT is largely derived by accessing computer-based sources, an argument might be made to have PACINT as a sub-discipline of SIGINT, with the computer network exploitation (CNE) mission under its portfolio. However, CNE is more specifically focused on obtaining access to closed or controlled networks that are designed to be inaccessible. PACINT is focused on what is readily available to the "crowds" in the public domain, not on restricted or closed systems. A more useful comparison to SIGINT is in the way information can be described as "externals" or "internals." SIGINT focusing on the communications hardware itself, whether it is a cell phone handset, a push-to-talk radio, or a high-powered cordless phone, is said to be focused on the "externals." Monitoring the "externals" provides a baseline for *how* targets are communicating. The "internals" focus on *what* the targets are specifically communicating. PACINT is focused on the *internals* to understand the social message that is providing the tipping point, but it is proactively monitoring the *externals* to determine how quickly the message is spreading and where through the public domain.

OSINT-derived information can come from academia, print media, radio broadcasts, and social networks. What is missing, though, is the application of those sources with socio-cultural underpinnings.

The idea of tapping into readily available public information is what also presents the largest challenge to PACINT becoming its own discipline—hence, the alternative argument that it already is or should become a sub-discipline of OSINT. A careful reading of JP 2-0 reveals that OSINT does not have sub-disciplines within it, but has multiple sources from which to obtain information. OSINT-derived information can come from academia, print media, radio broadcasts, and social networks. What is missing, though, is the application of those sources with socio-cultural underpinnings. Whereas the focus of PACINT is to provide situational awareness leading to strategic warning, OSINT primarily provides insight into "controlled" sources, and does not provide a "voice" of the people at large. In other words, the majority of OSINT by its design is not "crowd-sourced"; it is single-sourced from

a variety of venues. An analyst receives the perspective of a specific reporter, radio host, or scholar who may or may not have political agendas behind his or her statements, and who may or may not represent the pulse of the people at large. This approach is valuable as it typically does give additional insight into the perspective of the government or the military (within the Clausewitzian trinity). However, without providing "crowd-sourced" information, using OSINT products and sources does not provide analysts with the voice of the people. Even if OSINT does become savvy at providing crowd-sourced information in the future, that is not sufficient to make it PACINT. Understanding the underlying socio-cultural dynamics, the social triggers that lead to nation-state tipping points, and the capability to share information is also necessary to complete the new discipline's methodology.

PACINT IN ACTION

U.S. Southern Command's introduction to this new intelligence discipline first appeared during Operation UNIFIED RESPONSE (OUR), the humanitarian assistance and disaster relief mission to Haiti following the 12 January 2010 earthquake. Obtaining information within the first 48 hours was challenging due to the outage of cell phone communications, severing of the single undersea fiber-optic cable, and loss of power to Internet service providers (who primarily used satellites to provide global connectivity).[8] What emerged in the days that followed was to find out who required lifesaving water, food, medical, transport, or other lifesaving needs by whatever means possible. While full cellular communications were not reliable, SMS text messaging seemed largely unaffected and became a primary means of communication. Using this dynamically available medium, and understanding the socio-cultural context that Haitians were dependent on foreign assistance for the crisis, a non-governmental organization (NGO) worked with Digicell (the primary cell provider) to provide a free SMS code for people to pass their needs.[9] These messages became the most powerful means of sharing the "voice" of the people to not only the U.S., but to all nations involved in providing lifesaving humanitarian assistance where needed.

PACINT also proved useful during OUR as a critical "INT" in planning efforts to identify World Food Program distribution points. Crowd-sourced intelligence provided analysts the ability to identify the Haitian population's mobility status, access to cleared pathways, and needs for humanitarian relief distribution security. Additionally, as Internet and cell services became more reliable, the Haitian diaspora within South Florida began passing anecdotal reporting of needs throughout Haiti to help direct U.S. assistance efforts through social media sites. Since none of the traditional "INTs" categorically captured a way to obtain this crowd-sourced intelligence from multiple sources, SOUTHCOM recognized the need to develop processes to leverage this non-traditional ISR source. General Douglas Fraser, the SOUTHCOM Commander, publicly endorsed this approach "to analyze social media…so we can identify regional trends early and accurately" in testimony to Congress.[10] His comments came after a series of post-OUR events within the SOUTHCOM AOR provided opportunities to test PACINT on strategic warning problems.

Starting in November 2010, the turmoil leading up to the March 2011 Haitian elections and subsequent return of Jean-Claude "Baby Doc" Duvalier (President of Haiti 1971-86; fled Haiti following uprisings) and Jean-Bertrand Aristide (President of Haiti 1991 until removed through *coup d'etat*; returned to power 1994-96 following Operation UPHOLD DEMOCRACY; elected again in 2001 until resignation and exile in 2004) provided an opportunity to examine PACINT as a predictive method for strategic warning items of interest. Social media provided insight into the security requirements and protective measures required in a highly-charged political election season in a country with a history of instability during political uncertainty. Historically, Haitian civil strife has been a "push" factor to drive increased illegal migration toward the United States. Understanding whether or not the return of the former rulers, as well as the political elections, would result in strife that might directly affect U.S. national security interests was paramount.

Regarding Baby Doc's return, social media and networking sites provided an almost instantaneous source of "the people's" reaction. These sources surprisingly provided less focus on Duvalier's return and focused instead on the potential for the return of former President Aristide. Understanding the Haitian socio-cultural dynamics underpinned SOUTHCOM assessments that the current generation of Haitians (who frequented these social media sites) had few if any personal experiences with either Baby Doc or Aristide. This analysis resulted in predictive assessments characterizing the Haitian reaction as one of caution among the youth and not of explosive violence. Once Aristide's return was imminent, SOUTHCOM analysts reaffirmed earlier predictions that his arrival in Haiti would generate caution instead of widespread violent protests based on "the people" providing their "real-time" voice through social media feeds (e.g., radios, tweets, blogs, etc.). The end result netted successful use of PACINT-derived information to provide strategic warning on the likely stability of Haiti during a time of political uncertainty.

Two other events within the SOUTHCOM AOR advancing PACINT included the impact of Middle East/North Africa

uprisings on Latin America as well as recent protests in Bolivia. The revolts in Tunisia, Egypt, and Libya arguably had a social networking aspect to help mobilize the grassroots population. While the full extent of that influence is for other scholars to debate, the influence upon Latin America could not be ignored by SOUTHCOM analysts. PACINT provided information that similar protests were being called for in Cuba to oust the Castro regime via social media. However, analysts determined that the lack of socio-cultural triggers, a submissive population, the relatively unknown status of the organization calling for such protests, and the lack of dynamically available information to the target population (less than 3% have access to the Internet) made it unlikely a similar protest would happen in Cuba on the dates announced.[11] A maturing use of PACINT provided accurate strategic intelligence, based on the application of the dynamic availability, socio-cultural awareness, and crowd-sourced information analysis methodology.

The final example within recent months involves local protests within Bolivia over multiple unpopular decisions made by President Evo Morales. Protests within Bolivia cannot be taken lightly because on at least two occasions (in 2003 and 2005) they resulted in Bolivian presidents resigning from power. Instability of countries within the SOUTHCOM AOR can lead to other second- and third-order effects for the United States, such as increased illicit trafficking flow, which warrants attention as a heightened threat to national security. The first series of protests began in December 2010 over a decree to end fuel subsidies, which raised fuel prices over 70% with a simultaneous impact on food prices.[12] This "trigger" resulted in protests and strikes among transportation workers and bakers, illustrating how quickly a grassroots mobilization resulted in a crisis for the nation-state. National priorities limited traditional ISR available for this problem set. Therefore, an opportunity to apply PACINT principles became the method of choice to understand the extent of the movement and likely outcomes. Noting the rapid spread of the protest messages through social media, and the potential for violence in La Paz, El Alto, Santa Cruz, Oruro, and Cochabamba, it seemed clear, based on precedent, that Morales would be forced to resign unless he made concessions given the resonating social trigger. Within a week, President Morales reversed his decision, quelling the "population."

Four months later, a second event involved President Morales' decision to provide a 10% raise for teachers and health workers. In April 2001 the country's primary trade union federation called for protests to demand a 15% pay raise.[13] SOUTHCOM once again leveraged PACINT to provide insight into the situation to provide strategic warning to decision-makers on Bolivia's internal stability and outcomes that may present long-term strategic problems for the Morales administration. Analysts conducted a study on how many users had access to the Internet plus radio station affiliations, and began obtaining dynamic information from web sites associated with the protests. The initial results suggested lack of a grassroots mobilization among 18- to 24-year-olds based on social networking feeds. As such, analysts assessed the protest would likely end with the Bolivian government compromising with the trade unions, and Morales would remain in power. Although a few events cannot validate PACINT as part of a new methodology for strategic warning, the continued refinement of incorporating PACINT into multi-INT, all-source intelligence analysis will provide the foundation for establishing a new strategic warning framework for the 21st century.

TRANSFORMING THE 21ST CENTURY STRATEGIC WARNING FRAMEWORK

Traditional ISR has been able to address the capabilities and intent of U.S. adversaries throughout the 20th century. The focus of strategic warning on foreign governments and their militaries was justified given that nation-states were the primary actors on the global scene through the end of the Cold War. Now that irregular warfare has dominated the last 10 years of the U.S. national security effort, strategic warning as an art against traditional adversaries has eroded. However, going back to tried and true ISR assets to determine capabilities and intent is not sufficient as the global scene has shifted. There are certainly non-state actors who remain in the world that wish to do harm to the United States. However, a critical 21st century non-state actor that is ignored by traditional ISR is "the people." Grassroots social mobilization can create instability within a nation-state that can result in "stomping grounds" for violent extremists or other organizations to take advantage of uncertain security situations. The resulting lack of status quo security can create an environment where adversaries take the opportunity to cause economic or infrastructure damage that prolongs recovery, increase trafficking of illicit materials, raid the unstable country's weapons stockpiles (possibly including WMD), and increase their presence in the country to conduct attacks against any U.S. military personnel who may be called to respond.

Ignoring the people in the 21st century is too dangerous an option. Likewise, the strategic framework must also continue to incorporate the government and the military aspects of the Clausewitzian trinity since those institutions are likely to generate the socio-cultural triggers creating a change in the social landscape. Those triggers can be predicted by the U.S. IC if there is proper socio-cultural

awareness and analysis conducted as part of the Joint Intelligence Preparation of the Operational Environment (JIPOE) for global strategic analysis. Once these factors are understood, dynamically available social media can then be utilized to monitor for any population-driven movement that would result in a crisis for the nation-state of interest. The traditional INTs must still be utilized to build JIPOE to set the conditions for including PACINT effectively, as well as being able to visualize PACINT and the social movement effects geospatially. Specifically, the ability to layer information to show "hot spots" of activity in concert with socio-cultural linkages through a city, a region, and the globe will be key to future I&W efforts.

When combined with traditional INTs, PACINT allows for an evolutionary transformation concept where a traditionally ignored non-state actor, "the people," becomes a critical element of I&W instead of focusing primarily on governments and militaries. The IC is already overburdened with multiple requirements that cannot possibly be met with ISR assets on hand, but PACINT will utilize a global wide-area surveillance platform via existing technologies to support a 21st century strategic warning methodology.

FUTURE DEVELOPMENTS: AUTHORITIES, POLICIES, AND STANDARDS

Scholars interested in this nascent field need to research the application of Title 10 and Title 50 authorities, debate the pro's and con's of implementing PACINT policies, and identify architecture standards for this new discipline. The proper authorities will assist analysts in identification of hot issues, significant trends, and key social indicators that would threaten the status quo or create change rising to the nation–state level. Having the appropriate authorities to utilize these tools will enable predictability for certain messages to go "viral" within any country worldwide.

Intelligence oversight paradigms for the 21st century will likely need updating to better reflect the nature of social networking in that one cannot completely separate U.S. from non-U.S. persons.

A corollary to the authorities question is a need to understand the impact of implementing policies regarding PACINT collection, retention, and dissemination processes. While current guidance allows for PACINT, policies are not static. Intelligence oversight paradigms for the 21st century will likely need updating to better reflect the nature of social networking in that one cannot completely separate U.S. from non-U.S. persons. Additional research into potentially partnering with law enforcement agencies for sharing or storing these data may provide additional policies to make better use of PACINT in the long term.

A third area of research is required on how to best integrate PACINT into existing architecture standards. Today's collection management enterprise utilizes established processing, exploitation, and dissemination frameworks, such as the Distributed Common Ground System, to transmit and share all-source intelligence. The intent of integrating PACINT into the existing architecture is to create a passive system that has "active" requirements to generate data while ensuring the free flow of information by avoiding the proliferation of disparate proprietary systems and methods, which has plagued previous sensor integration. Establishing standards and protocols to allow integration of existing data and tools, rather than creating new information technology backbones or structures, will make more efficient use of taxpayer dollars.

SUMMARY

In an era of cost-saving efficiencies, declining resources, and ongoing worldwide priorities, the PACINT concept provides an effective method of generating timely, predictive intelligence through a global wide-area surveillance platform without the need to invest in high-dollar collection systems. The 21st century has provided the people with a voice to express their own views and expressions at a speed never seen before in history due to global communications connectivity. The people themselves can finally be considered a viable non-state actor who can generate protests, instigate riots, and potentially alter or at its extreme take down governments, all of which may have second- and third-order effects for the United States.

The IC must transform itself to capture this non-state actor's influence to bring strategic warning back to the acute, heightened status it once held during the Cold War. It will not be the same type of strategic warning, nor will it necessarily be conducted at the national level. Instead, analysts will utilize dynamically available social media, underpinned by knowledge of socio-cultural conditions and triggers, to generate crowd-sourced intelligence aimed at understanding "the people" as a non-state actor. These tenets of PACINT, as evidenced through events in SOUTHCOM, illustrate why it deserves consideration as a new intelligence discipline. This intelligence discipline will be repeatable, predictable, and verifiable so that personnel can be trained, collection requirements can be

submitted, and sources can be characterized. A concerted effort by the IC to establish appropriate authorities, policies, and standards will validate PACINT as a legitimate field to provide decision-makers real-time information as part of a new 21st century strategic warning methodology.

Notes

[1] Colonel T.X. Hammes, USMC (Retired), "Fourth Generation Warfare Evolves, Fifth Emerges," *Military Review* (May-June 2007), 14-23, <http://www.au.af.mil/au/awc/awcgate/milreview/hammes-4gw_and-5th.pdf> (accessed 24 April 2011). Hammes does credit that in 5GW "networks will distribute the key information, provide a source for the necessary equipment and material, and constitute a field from which to recruit volunteers."

[2] Karl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 89. There has been scholarly debate on whether the Clausewitzian trinity specifically referred to the people, the army, and the government or whether these were mere examples of his trinity. This paper does not seek to add to that debate, and considers the "trinity" as the people, military, and government. See Christopher Bassford and Edward J. Villacres, "Reclaiming the Clausewitzian Trinity,"*Parameters* (Autumn 1995), for alternative views.

[3] MG Michael T. Flynn, Capt Matt Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington, DC: Center for New American Security, January 2010), 23, <http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf> (accessed 24 April 2011).

[4] See Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 3rd ed. (Washington, DC: CQ Press, 2006), for an excellent summary of intelligence disciplines and some general history behind each one. [Editor's Note: The updated 4th edition of this seminal text was published in 2009.] [5] Stephen C. Mercado, "Sailing the Sea of OSINT in the Information Age," *Studies in Intelligence* 48, no. 3 (2004), <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html#author1> (accessed 24 April 2011).

[6] Paul Wood, "Afghanistan: Deadly Kandahar Protest at Koran Burning," *BBC News Online*, 2 April 2011, <http://www.bbc.co.uk/news/world-south-asia-12944851> (accessed 24 April 2011).

[7] See Everett M. Rogers, *Diffusion of Innovations*, 5th ed. (New York: Free Press, 2003).

[8] "Haiti's Only Direct Submarine Cable Disrupted, but Most ISPs Operational," *Telegeography.com*, 15 January 2010, <http://www.telegeography.com/products/commsupdate/articles/2010/01/15/haitis-only-direct-submarine-cable-disrupted-but-most-isps-operational/> (accessed 24 April 2011).

[9] "SMS Shortcode Helps Haiti's Relief Effort," *Channel 4 News Online*, 18 January 2010, <http://www.channel4.com/news/articles/arts_entertainment/media/sms+shortcode+helps+haitiaposs+relief+effort/3506057.html> (accessed 24 April 2011).

[10] Marcus Weisgerber, "U.S. SOUTHCOM Adds Twitter to ISR Toolbox," *Defense News* (5 April 2011), <http://www.defensenews.com/story.php?i=6154210&c=policy.%20land,%20air,%20naval&s=TOP> (accessed 24 April 2011).

[11] Juan O. Tamayo, "Calls for Egypt-like Riots in Cuba Not Getting Support," *Miami Herald*, 3 February 2011, <http://www.miamiherald.com/2011/02/03/2047990/egypt-like-riots-not-likely-at.html> (accessed 24 April 2011). Vanessa Lopez, *The Venezuelan-Cuban Fiber Optic Cable: A Connection to the World?* (Miami: Institute for Cuban and Cuban-American Studies), 1 March 2011, <http://ctp.iccas.miami.edu/FOCUS_Web/Issue138.htm> (accessed 24 April 2011).

[12] "Bolivia's Morales Drops Planned Fuel Prices Hike," *BBC News Online*, 1 January 2011, <http://www.bbc.co.uk/news/world-latin-america-12101199> (accessed 24 April 2011).

[13] "Bolivia Protests Challenge Evo Morales," *BBC Online*, 15 April 2011, <http://www.bbc.co.uk/news/world-latin-america-13099827> (accessed 24 April 2011).

Brig Gen (USAF) Dash Jamieson is the J2, Director of Intelligence, Surveillance, and Reconnaissance, for U.S. Southern Command. She is responsible for planning, directing, and synchronizing joint ISR analysis and operations in coordination with partner nations in Central and South America and the Caribbean. She led the SOUTHCOM J2 Directorate during Operation UNIFIED RESPONSE, where she first identified PACINT as a potential intelligence discipline warranting discussion. She is a 2004 graduate of the National War College.

Lt Col (USAF) Maurizio "Mo" Calabrese is the Chief of ISR Collection Management for U.S. Southern Command. He is responsible for theater ISR collection requirements, operations, and assessments. He is a 2008 graduate of the National Defense Intelligence College and a recipient of the U.S. Coast Guard Foundation's Elizebeth Friedman Award for his thesis work on pyro-terrorism as an asymmetric weapon of mass destruction in the homeland.

Sensemaking:
A Transformative Paradigm

by David T. Moore
and Robert R. Hoffman

The opinions expressed in this article are those of the authors. They do not reflect the opinions of the National Security Agency, the Department of Defense, the Office of the Director of National Intelligence, or the U.S. Government. No inferences of official or unofficial policies or plans of the National Security Agency, the Department of Defense, the Office of the Director of National Intelligence, or the U.S. Government should be construed from this article. Approved for unlimited release, PP-11-0116.

Portions of this article are drawn from Sensemaking: A Structure for an Intelligence Revolution (Washington DC: NDIC Press, 2011). Cited hereafter as Moore, Sensemaking.

INTRODUCTION

Intelligence remains broken in ways that legislation and technology alone cannot fix.[1] Indeed, the search for technological fixes may lull Intelligence Community management and its overseers into a false sense of confidence that it has met and exceeded the legislated reforms. In other domains, notably economics, such confidence is described as a "bubble." And as the nation (and world) repeatedly has seen, bubbles eventually burst.[2] When intelligence bubbles burst, the results can be catastrophic as was seen in 1941 as well as 2001. We fear the next burst intelligence bubble could well be worse than those of the past. Such considerations beg the question, what is that underlying problem with intelligence? This question also leads one to ask, what are alternative paths to a fix that works? These are the two key questions of this article.

Our view is that the present "reforms" likely will not get us sufficiently far to meet the intelligence challenges of the 21st century.

A decade ago when one of us (Moore) began to examine critical thinking as a means of improving what intelligence professionals do, he recognized that a critical thinking approach could lead in novel directions as issues and problems were considered from different perspectives.[3] At the same time, he began to have doubts about what is meant by "intelligence reform," in any pragmatic sense. Were the reforms of that (and the present) decade really about improving what is being created or protecting the community?[4] This led to discussions with his coauthor and this article. Our view is that, depending on how they are conceived, the present "reforms" likely will not get us sufficiently far to meet the intelligence challenges of the 21st century.

Both of us have spent years examining how people reason, especially experts. Research shows that, as a means of reasoning, "sensemaking" done well leads to sound decision-making. Given our differing professions we each define the concept of sensemaking somewhat differently. Both of us have been informed by the work of Karl Weick and Brenda Dervin.[5] Karl Weick sees sensemaking as a multiple-step process by which someone goes from becoming aware of "something, in an ongoing flow of events, something in the form of a surprise, a discrepant set of cues, [or] something that does not fit," to a useful understanding of the phenomenon.[6]

According to Dervin, sensemaking is "a set of philosophical assumptions, substantive propositions, methodological framings, and methods."[7] Working from the point of view of the intelligence professional, Moore defines sensemaking as an approach that involves planning and replanning about how to make sense of an issue; foraging for, and harvesting sources of information; seeking to understand what they reveal; and communicating that knowledge to others.[8]

Hoffman considers sensemaking to be one of the fundamental processes of "macrocognition," defined as the adaptation of cognition to complexity. Working with Gary Klein (and others), he has advanced a general model of sensemaking, which we present and rely upon in this article. The Data/Frame Model of Sensemaking describes how experts actually reason. We suggest that, when applied to a practice of intelligence, it offers answers to our two key questions.

As a part of this discussion we examine the differences between reform and another concept – transformation. We offer a comparative look at two paradigms for intelligence – those of Sherman Kent and Willmoore Kendall. Kent's model is close to what is actually practiced today. Kendall's seems to be more in line with what we believe is needed. Indeed, Kendall's model dovetails with the macrocognitive approach. Analytical or critical thinking is not thought of as a sequence of stages that magically turn data into wisdom, and from that achieve some singular goal of calculating outcome probabilities. Rather, cognition is seen for what it is – a continuous flux of multiple processes including problem detection, mental model formation, projection to the future, replanning, and others. Macrocognitive processes are continuous, parallel, and highly interacting. It is only by recognizing this fact, and pursuing its implications, that we might achieve a genuine understanding of intelligence phenomena. We believe such a sensemaking approach will guide us in meeting the challenges posed to intelligence professionals of this century.

REFORMATION VERSUS TRANSFORMATION

We begin with an observation by systems theorist Russell Ackoff about the differences between reformation and transformation. Despite his critical impact on several key disciplines, Ackoff is not a household name even among the cognoscenti. Hence, a bit of an introduction of him is in order. Russell Lincoln Ackoff (12 February 1919 – 29 October 2009) was an American organizational theorist, consultant, and Anheuser-Busch Professor Emeritus of Management Science at the Wharton School, University of Pennsylvania.[9] The author of 25 books (two published posthumously) and numerous articles, Ackoff was a pioneer in the field of operations research, "systems thinking," and management science. He stated: "Reformations and transformations are not the same thing…. Reformations are concerned with changing the means systems employ to pursue their objectives."[10] In contrast, "Transformations involve changes in the *objectives* they pursue... there is a difference between doing things right (the intent of reformations) and doing the right thing (the intent of transformations)."[11]

We have been reforming intelligence for nearly 70 years and are still making the same kinds of mistakes summarized by overseers as "failures of imagination" and failures to "connect the dots."[12] We have focused on the *means* by which we are organized and more recently the means by which we do "analysis." Bruce Chew, of the consulting firm Monitor 360, observes that repeated failures can be symptomatic of organizational failure.[13] Pessimists such as Richard Betts tell us such is the nature of intelligence work.[14] If Betts is right, then we might as well shut down our Community education and training institutions. Why educate and train our new intelligence creators if they are doomed to fail?

We prefer a more hopeful outlook and seek a positive portrait of analyst cognition, not one that is characterized by failures and biases. We are and remain meliorists (although at least one of us is a skeptical meliorist). Things do not have to be the way they are. Intelligence can be improved. However, if, as the record makes clear, and despite our best efforts, we continue to be unsuccessful in our attempts to reform (in other words, fix) intelligence, then Chew's observation is right with regard to intelligence: We must conclude our problems are systemic. Thus we need to transform intelligence; we must envision intelligence anew.

Revolution means a new paradigm, as Thomas Kuhn observed about transforming normal science.

Ackoff points out that reformations only change the *means* systems employ to pursue their objectives, whereas transformation is a revolutionary process. To reiterate, therefore, perhaps the time is right to consider a revolution in intelligence.[15] Revolution means a new paradigm, as Thomas Kuhn observed about transforming normal science.[16]

INTELLIGENCE NOT THE (SOLE) PRODUCT OF ANALYSIS

The late Dr. Mark Weisenbloom, formerly of the Joint Military Intelligence College (now the National Defense Intelligence College),[17] used to socratically challenge new students in that institution's Master of Science of Strategic Intelligence program to explain what intelligence is.[18] Part of that discussion revolved around what it is that people do when they create intelligence. He challenged his students with the idea that "analysis" meant disaggregation and that was not, in fact, what intelligence professionals did. The lecture was challenging for him, since his students often did not "get it." The lecture also was challenging for his students because they simply did not get it.

This begs the question: What kind of an intelligence discipline does the Community possess if it cannot accurately and precisely characterize what it does? This is a germane question as intelligence analysis currently is not formally regarded as a profession. According to the Office

of Personnel Management, intelligence is an administrative function.[19] Therefore, the belief that we currently represent a profession is arguably a fiction. Nevertheless, we argue it could and should be a profession. Getting the paradigm right is a necessary first step. So, what is it that we actually do?

> ***Analysis is* not *what we do – or at least not all that we do. We also simultaneously and sequentially synthesize, interpret, and communicate the results of our thinking about sparse and noisy, uncertain data to somewhat interested individuals and organizations. This aggregate of processes and functions has a name. It is sensemaking.***

The question Weisenbloom asked is essential, because analysis is *not* what we do – or at least not all that we do. We also simultaneously and sequentially synthesize, interpret, and communicate the results of our thinking about sparse and noisy, uncertain data to somewhat interested individuals and organizations. This aggregate of processes and functions has a name. It is sensemaking.[20] Sensemaking, according to Xerox PARC innovator Mark Stefik, "is how we gain a necessary understanding of [the] relevant parts of our world."[21] Intelligence sensemaking "encompasses the processes by which specialized knowledge about ambiguous, complex, and uncertain issues is created" (again) from noisy, sparse, and uncertain data such as that with which we routinely work.[22] Such work, according to information science expert Peter Pirolli and evidence-expert David Schum, and the present authors, involves planning and replanning, foraging, marshaling, understanding, and communicating.[23]

One model of sensemaking is presented in the figure. This model derives from studies of expert decision-makers in diverse domains, ranging from business leaders to military commanders.[24] The starting point is recognition of a situation or a problem, which is understood in terms of some sort of framework or story. The determination of an initial frame for understanding is not a bias. Rather, it is a necessary first step in making sense of things, as one asks, "What's going on in this situation?" Following the comprehension of data and formation of an initial frame, there are alternative paths that involve either elaborating a frame, questioning a frame, or forming an alternative frame. We invite the reader to ponder ways in which this fits his or her own reasoning about analytical problems.

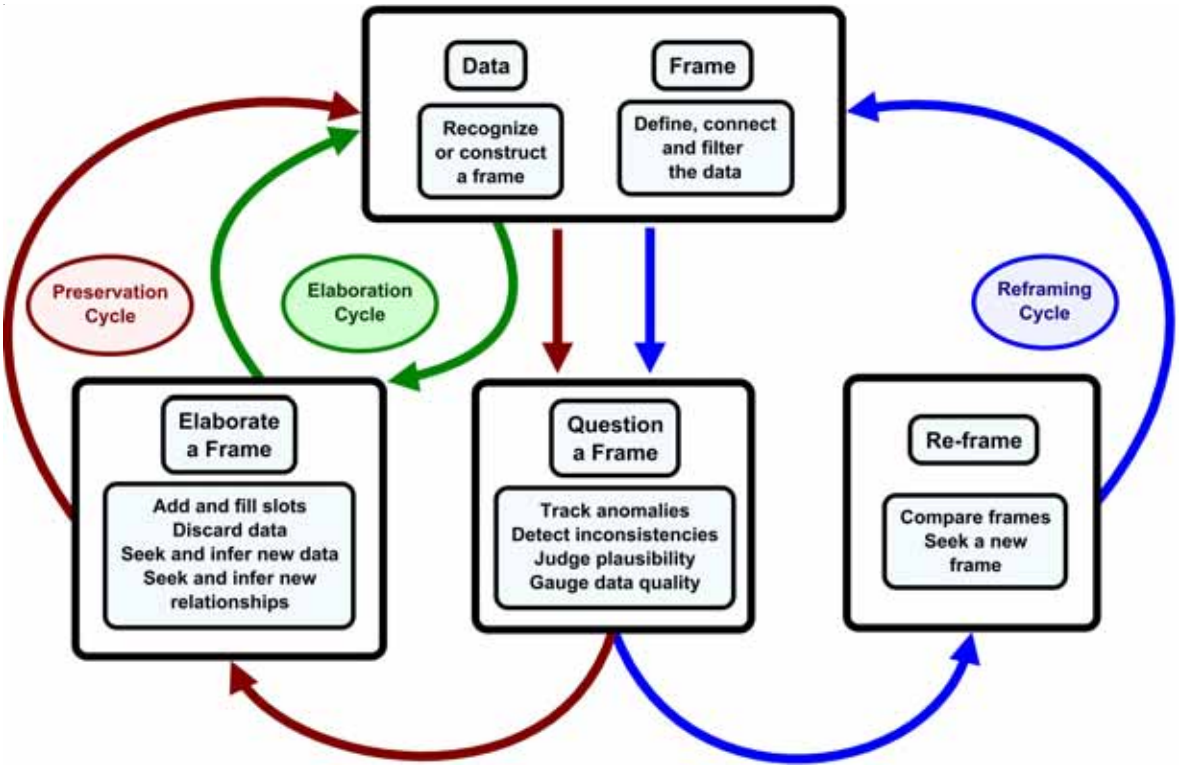


Figure: Data-Frame Theory of Sensemaking
Source: Authors

What we would like to note about this model is that there is no single "exit" point, when an analysis is done. A second key point is that the frame for sensemaking determines what counts as data. An example is the search for the cause of AIDS. At first, it seemed to be a rare form of cancer, and then it became clearer that what the AIDS "effect" explained was why gay men were dying of infectious diseases. As the investigation continued, the perceived effect morphed to include intravenous drug users, then also people who had received blood transfusions, and other at-risk populations. Eventually the search for data led to the current frame: AIDS is a set of diseases arising from a virus that attacks the human immune system.

"[A]nalysis" as a term for what we do is neither sufficiently precise nor, for that matter, accurate.

Why is this notion of "intelligence sensemaking" versus "intelligence analysis" more than merely a semantic matter? The answer to this question has to do with the nature of the transformations in the intelligence community that seem to be called for. Einstein expressed our point when he noted that "without changing our patterns of thought we will not be able to solve the problems we created with our current patterns of thought."[25] Gerald Nosich believes (based on many years of trying to help people improve their thinking) that "changing our thinking requires changing our vocabulary."[26] If, therefore, we need to transform how we do intelligence we need to change our thinking about intelligence. To do so means we need to also change our vocabulary. We need a different set of paradigmatic conceptual terms. In sum, "analysis" as a term for what we do is neither sufficiently precise nor, for that matter, accurate.

PUZZLES, MYSTERIES, AND MORE

In the world of the nation-state, Gregory Treverton and others divided intelligence problems into puzzles and mysteries (or variants of those words).[27] Puzzles are those questions that have – at least in principle – a single, definitive answer. What make puzzles hard is that we often make false assumptions about them. As Ackoff notes, such an "incorrect assumption…precludes a solution."[28] Treverton considered that "how many nuclear missiles the Soviet Union had during the Cold War [was] a puzzle. So is whether Al Qaeda currently possesses fissile material."[29] Evidence needed to answer those problems is at least theoretically knowable although it likely is unknown and certainly is hard to obtain. With puzzles an answer is obtainable – although the cost may be excessive.

By contrast, Treverton asserts "mysteries are questions that cannot be answered with certainty. They are future and contingent. Will North Korea reach agreement to quit its nuclear weapons program? No one knows the answer, not even North Korean leader Kim Jong Il."[30] Evidence is unknown and likely unknowable. The question is a mystery, not a puzzle. Seen in foresight there is no one single answer, and uncertainty surrounds each possible answer. We continue to face both puzzles and mysteries today.

However, we also face a third kind of phenomenon in a world where nation-states are no longer the principal actors. Today's transnational threats confront us with something more than mysteries. Treverton calls these "complexities," borrowing a term developed by David Snowden.[31] They also are sometimes called "wicked problems" or "social messes."[32] Treverton notes the following:

> They come without history or shape. Large numbers of relatively small actors respond to a shifting set of situational factors. Thus, they do not necessarily repeat in any established pattern and are not amenable to predictive analysis in the same way as mysteries. These characteristics describe many transnational targets, like terrorists – small groups forming and reforming, seeking to find vulnerabilities, thus adapting constantly, and interacting in ways that may be new.[33]

We only pretend to answer or solve these types of issues: They do not have single, determinate solutions. Indeed, when we pose what we call "solutions," we invite unanticipated and undesirable consequences as those solutions are implemented by policymakers.[34] The issues themselves are shorthand references to larger complex and adaptive systems. Further, they react to our actions. But we can – within some bounds – make sense of these kinds of issues. The sense we make may allow policymakers to steer relevant actors to some mutual goals.

Considering both problem types and the problems themselves is a useful meta-process that provides insights into the mechanics of how we actually make sense of phenomena. This is useful as intelligence often finds itself in a similar position to medicine in the 15th century. In this latter case we know what to do with a gut wound; we simply pack it full of moss. If the patient lives, the technique worked. If the patient dies, well, that occurred not because the technique did not work but rather because God willed it otherwise.

Using a macrocognitive model of sensemaking also is a manifestation of critical thinking. It involves reflecting on

what one is doing – an important part of the process. Additionally, engaging in critical thinking (self-consciously and systematically seeking to understand the what-and-why of a phenomenon, the varying perspectives, evidence and inferences, implications and alternatives) provides a rigor that helps ensure the issue is as thoroughly understood as feasible.

Sensemaking also requires an attitude of mindfulness.

Sensemaking also requires an attitude of mindfulness. We need to be aware of what is going on around us if we are going to make sense of it. Mindfulness for social-psychologist Ellen Langer involves "[an aptitude for the] creation of new categories; openness to new information; and…awareness of more than one perspective."[35] The idea that "[a] steer is a steak to a rancher, a sacred object to a Hindu, and a collection of genes and proteins to a molecular biologist" is one with which sensemakers will be comfortable.[36]

Consider, for example, the counterterror professional who is mindfully considering who might be a member of Al Qaeda. Continuously with that, and in parallel, there is a process of uncertainty management about who might hold such membership, and a process of conceiving of paths to new information for making sense of the organization and its membership. Such considerations prime the intelligence professional to consider that people not normally associated with Al Qaeda—such as an American woman from Pennsylvania—might be sympathizers or even members.

Mindfulness has another dimension as well. Mindful consideration of complexities (as well as puzzles and mysteries) means one is not looking merely at the bright and shiny factors of the issue—perhaps the immediate threat perceived of a group of violent non-state actors—but also at the small elements and indicators that might presage a crisis or a catastrophe. Thus, in this macrocognitive approach intelligence sensemakers can create and become part of a resilient and highly reliable organization. Resilience is about changing how you operate once you have moved beyond your resources and competence envelope.[37] This is different from adaptation, in which you recover from problems that fall near the borders of your competence envelope but do not have to change how you do business in any fundamental way.

NOT A NEW PARADIGM

It seems that such a paradigm as we propose is not new, although it so far has been only sporadically applied in the Community. In the 1940s two different paradigms for intelligence were discussed in the context of the one that was widely adopted – those of Sherman Kent and Willmoore Kendall. Kent enduringly characterized a paradigm for intelligence over 60 years ago and it is still the principal model being applied in a world that is now very different in terms of the intelligence problems it poses.[38] His is the paradigm for normal intelligence, i.e., puzzle-solving. To Kent intelligence was a fact-finding process employing cumulatively researched tidal waves of previously collected data and information.[39] There was one correct answer that was suitably qualified with probabilities. In his view, the course of events was a tape and all you had to do is figure out how to read it.[40] It is a view that presumed all we need is sufficient data fed into the right elite minds and out would come the truths spoken to power.

When we take an empirical perspective and ask what we really do, however, we really do not speak truth to power. Rather it goes to an intermediary – often only a briefer who speaks it to power: Intelligence professionals are often kept separate from the policymaker.

Kent believed intelligence was created by elites. Logically, the more elite the analyst, the easier it was (and is) to read the tape. Could this be why some policymakers or their staffs (i.e., the most elite) prefer the raw data and wish to make direct sense of it? Finally, in Kent's view there is one answer, and who better than the consumers to determine what that answer is, since they have access to much more knowledge than that merely provided by intelligence.

We actually do not know how well this paradigm worked in Kent's day. Repeated intelligence errors and failures certainly make clear that the approach has not been perfect over the years.[41] Most famously the Kent paradigm did not work in 1962 when Kent informed the Community of his day that the Soviet Union would never place strategic nuclear missiles in Cuba. In defending his judgment, Kent noted "the—to us—incredible wrongness of the Soviet decision to put the missiles into Cuba," indicating the estimate was actually correct and the Soviet government acted improperly (differently than it should have) – in effect, God willed it otherwise.[42]

By contrast we have Kendall's paradigm, where the course of events is something you try to influence favorably. Intelligence, according to Kendall, attempts to understand how humans behave and think, and employs both

information and theory to make sense of complexities as well as puzzles and mysteries. More data may be helpful but also may not be necessary – something that was shown to be important by Paul Slovic nearly 40 years ago: Slovic found that more data can actually detract from accuracy.[43]

One reason for this is that there are a number of conditionally anticipatory answers, and more data can lead one further away from choice of effective action, not closer to it.

By contrast, in Kendall's model, an embedded intelligence professional paints a picture of the current situation and its possible futures to a senior official who provides feedback that further focuses the efforts of intelligence. Kendall's 60-year-old vision for intelligence is eerily close to that tied to a revolutionary paradigm of mindful strategic intelligence sensemaking, which we are advocating. We turn next to an explanation of the processes used by such an approach.

EMBODYING KENDALL: SENSEMAKING WITH A DATA/FRAME MODEL

A data/frame model of sensemaking provides insight into how people come to sound decisions. A practice of intelligence based on sensemaking is always forward-looking, into the hypothetical and possible future. Intelligence professionals engage in the creation of mental models of situations and the mental projection of those mental models into the future (see figure). These high-level functions allow cognition to adapt to complexity, and are distinguished from microcognitive processes such as millisecond-scale shifts of attention or access to long-term memory. In other words, macrocognition describes the cognitive processes that occur in the "real world" and which must be "successfully accomplished to perform a task or achieve a goal."[44] In the context of intelligence sensemaking, macrocognition focuses on what intelligence professionals *actually* do when they are making sense of an issue versus what they proscriptively should do (e.g., probability-juggling). Gary Klein and others observe a set of key features of macrocognition that typify the environment within which intelligence professionals struggle to make sense of things:

> Decisions are typically complex, often involving data overload. Decisions are often made under time pressure and involve high stakes and high risk. Goals are sometimes ill-defined, and multiple goals often conflict. Decisions must be made under conditions in which few things can be controlled or manipulated; indeed, many key variables and their interactions are not even fully understood.[45]

One of the most important tenets of macrocognition—some might say one of its most radical tenets—is that mental processes such as uncertainty management, creating mental models, maintaining common ground, and others, are always continuous, parallel, and highly interacting. No simple cause-effect chain theory of cognition, of the sort common to information processing approaches, will suffice at the macroscale. The processes of macrocognition lie at the heart of what it is that we do whether it involves constantly updating our mental models about an apparent aquatic fowl observed on a lake, an emerging weather condition, or who constitutes a member of a terrorist organization and the threat he/she may pose if allowed to board an airplane. Such processes are useful in dealing with intelligence puzzles and mysteries that typified Cold War intelligence. They become critical when it comes to making sense of the complex issues of the post-Cold War environment, as will be discussed next.

GETTING THERE

Monitor 360 futurists Doug Randall and Peter Schwartz believe that to be successful against strategic surprise – a goal the IC seeks – organizations must be both imaginative and systematic. While we assert elsewhere—based on extensive examination of failed and successful examples—that predictions made by flipping a coin often have a greater chance of coming true than those of the futurists, we do acknowledge that anticipating strategic surprise can be successful. We believe this in part because "[one] cannot foresee strategic surprise without being imaginative… [and] the results will not be believable without being systematic."[46] If intelligence is to rise above the noise and get the attention of policy and then be acted upon, it must be both. As we develop in detail elsewhere, a critical, mindful process of sensemaking offers a means for this to occur because it covers issues broadly, takes into account their complexity, and is systematic and rigorous. It offers the best means currently understood for making sense of what is known, knowable, and even what is unknown (transforming it at best to a "known unknown" and, at worst, to a "knowable unknown").

Engaging in macrocognitive sensemaking, with its multiple foci of (re)planning for problem detection, use of leverage points in constructing options, and management of both attention and uncertainty, further creates an approach that will improve communication with consumers of intelligence.[47] It reduces the nonsense of which Gary Zukav writes as he notes that "[nonsense] is nonsense only when we have not yet found that point of view from which it makes sense."[48] Such an inclusive sensemaking process provides that point – or rather *points* – of view; nonsense is

transformed into vital, strategic, and foresightful knowledge facilitating better decisions by leaders.

One of Treverton's shapeless complexities would be the emerging roles of non-state actors. If you doubt that they are emerging as very significant players within a very wicked problem set, consider not only Al Qaeda – which is a non-state actor – but Julian Paul Assange. Consider how he as a non-state actor has tied up and diverted the focus of the IC, the larger U.S. government, and the governments of several of our allies with his WikiLeaks releases of classified documents. As a recent case study into the emerging roles of non-state actors illustrates, there is no single answer to the question of the emerging roles of non-state actors.[49] Nonetheless, a sensemaking approach involving a multi-pronged, multi-discipline effort provides hope for a better understanding of the complexity that non-state actors represent. Such efforts do not – nor are they intended to – provide insights into precisely when and where non-state actors will strike next. They might, however yield insights into the conditions and circumstances where they might strike, allowing increased (and mindful) vigilance. Such a case study is additionally useful because it partially illustrates how we can begin to figure out what it is we really do, why it works or does not work, and how this informs our practice.

TRANSFORM OR ELSE

What are our options? Ackoff notes:

> The righter we do the wrong thing, the wronger we become. When we make a mistake doing the wrong thing and correct it, we become wronger. When we make a mistake doing the right thing and correct it, we become righter. Therefore, it is better to do the right thing wrong than the wrong thing right.[50]

If a reform model cannot fix intelligence then we are left with a model of transformation. A mindful *sensemaking* approach enables the intense, holistic scrutiny of complex developing scenarios and provides a paradigm where we can do the right thing. Such a macrocognitive approach ensures that the knowledge created also evolves. While it is true that sensemaking could be used as a method of reform – in a "cookbook" recipe fashion, it is best regarded as a transformational approach. It changes, when applied within the Kendallian model the objectives of intelligence – creating that transformation.

What are our options? Our only option is to transform. Reform fails and continues to fail where it really matters. For the IC to remain unchanged is not an option: the implications of error and failure are too dire. Further, we may not survive and will unlikely be allowed to survive another intelligence failure leading to a catastrophic disaster. Transforming intelligence, not reforming it, is our only course of action given the national security challenges of the 21st century. Mindful sensemaking represents a means of doing so. The macrocognitive practice orients us toward a professional practice of intelligence, based on our best knowledge of how real-world expert decision-makers actually reason in the face of complexity and uncertainty. We have a chance of doing the right thing as an intelligence enterprise – perhaps for the first and last time.

WHERE THE RUBBER MEETS THE TOAD

It is also important to note that frames describe the perceiver's understanding. "A frame is that portion of the perceptual cycle that is internal to the perceiver, modifiable by experience, and specific to what is being perceived."[51] As Klein and others note:

> Sensemaking begins when someone experiences a surprise or perceives an inadequacy in the existing frame and the existing perception of relevant data. The active exploration proceeds in both directions, to improve or replace the frame and to obtain more relevant data. The active exploration of an environment, conducted for a purpose, reminds us that sensemaking is an active process and not the passive receipt and combination of messages.
>
> People explore their environment by attending to a small portion of the available information. The data identify the relevant frame, and the frame determines which data are noticed. *Neither of these comes first*. The data elicit and help to construct the frame; the frame defines, connects, and filters the data.…[52]

It is also important to note that frames describe the perceiver's understanding. "A frame is that portion of the perceptual cycle that is internal to the perceiver, modifiable by experience, and specific to what is being perceived."[53] Once a frame is established, people "can't *not* see it."[54] Therefore, care must be exercised to ensure critical questioning of the frame and one's beliefs about it occurs. This is also necessary because frames and the data that describe them are highly interactive. Each informs and elaborates the other: People fit data into a frame and they fit frames around the data.[55] They do so by a variety of simplifying heuristics that simplify the reality of the world in which they operate and are based on their differing points of view.[56]

An example lies in the consideration of how intelligence could increase border security. If one approaches this situation from the perspective of counterterrorism, one might see border crossings as conduits for introducing terrorists into the country. From a counter-trafficking perspective, one would see them as places where narcotics and other desired consumable commodities are transferred, or where people bound for the sex-trade cross.

A danger arises if one is too wedded to a frame in that one will exclude others of equal or even greater likelihood.[57] One's perception is skewed and, as Richards Heuer writes, such

> circumstances under which accurate perception is most difficult are exactly the circumstances under which intelligence analysis is generally conducted – dealing with highly ambiguous situations on the basis of information that is processed incrementally under pressure for early judgment.[58]

Compounding this is the fact that different consumers of intelligence about the border also have different pre-existing frames. All may cling to different frames regarding what to do about the situation. The key is that all the frames might be correct, some of the frames might be correct, or none of them might be correct. It is the job of the intelligence professional to ascertain (admittedly with some degree of uncertainty) which is which *and* to stay open to the possibility that another interpretation of the data – in other words, another frame – might be exclusively valid or be equally valid. The critical thinking approach widely adopted by the Community – while difficult – emphasizes formally dissecting one's thinking about an issue and formally considering alternative explanations of that issue, i.e., reframing the issue. [59]

The data/frame model of Klein et alia also provides insight into the differences between novices and experts. While both novices and experts can employ the same strategies of reasoning, one thing that differentiates the two groups is that experts have a far richer set of narratives and perspectives on which they can comparatively draw than do the novices.[60] Such differences explain why experts make the connections to explain a phenomenon with which novices, who lack those connections, struggle. Certainly, any frame allows for the possibility that the reasoner may be blinded to alternative realities but, rather than seeing this as an inevitable bias, Data/Frame Theory sees it as an inevitable function in sensemaking. Thus, another distinction is that experts know that their frames offer singular perspectives and can deliberately question a frame and engage in re-framing. This skill is one that novices, almost by definition, lack.

Consider a situation where experts and novices each maintain a frame about the existence of an adversary's Weapons of Mass Destruction (WMD) program. The experts might view a purchase of aluminum tubes – despite an improper assay – as part of that program. Novices with little knowledge might not know to question the assay of those purchased aluminum tubes and be directed to find evidence of a WMD program which might link them to that program.

Thus, in this case the experts exhibit a sin of commission (they could challenge the frame but chose not to do so) and novices exhibit one of omission (they do not know to challenge the frame). In either case the frame is not challenged. Since in this example the consumer is also already predisposed toward finding evidence of a WMD program, the chosen frame justifies a policy to invade the country in question in order to put an end to this threatening program.

The Data/Frame Theory should entail specific guidance about how to engage an analytical process. The processes of questioning a frame, comparing multiple frames, and asking "what-if" questions can be seen in a number of descriptions of specific analytical procedures that have been recommended by intelligence professionals.[61] This being said, the Data/Frame Theory and macrocognitive approach do not mandate or emphasize a process of formulating hypotheses and assessing probabilities for the sake of mitigating bias. Methods that are more aligned with the positive outlook of Data/Frame Theory and the macrocognitive approach are those that emphasize collaboration, question generation, and challenge techniques. Clearly, this reconsideration of the "palette" of analytical methods is open with possibilities for further refinement.

The open possibilities reach all the way to taking seriously the individual differences in reasoning styles. Some analysts do not care for structured techniques, such as matrix-based evaluation or utility analysis. They prefer to immerse themselves in the evidence and let ideas percolate. Others seem to be driven by the need to continuously learn more and more about more and more. Yet, still others seem driven primarily by a need to create elaborate conceptual networks of interdependent propositions. We think it likely that paths through the Data/Frame process differ significantly as a function of reasoning style. Therefore, the question of "How should I best make sense of intelligence puzzles, mysteries, and complexities?" will not have a single answer: all three approaches will be valid in certain contexts.

One step, therefore, in transforming intelligence is to learn more about exactly what it is that has to be transformed. In

this context, if the macrocognitive approach has any value, we hope that it is to motivate programs of research into reasoning and reasoning styles, across the span of proficiency from apprentice to expert, so that we can have a solid empirical base on what it is that analysts actually do. By better understanding how we reason (and need to reason) we suggest we will better be able to reason about the complex issues of the 21st century.

Notes

[1] For a critical examination of the American preference for technology-based intelligence, see Kristie Macrakis, "Technophilic Hubris and Espionage Styles during the Cold War," *Isis*, vol. 101, no. 2 (June 2010), 378–385.

[2] In the above-mentioned economics example, this led to loss of prosperity, shelter, health, and way of life. Such losses also may have contributed to tragic loss of life. In the United States the scale of fatalities remained small—due in part to greater resilience in the American social fabric.

[3] David T. Moore, *Critical Thinking for Intelligence Analysis* (Washington, DC: NDIC Press, 2007), and Robert R. Hoffman, Brian Moon, David T. Moore, and J.A. Litman, "Reasoning difficulty in analytical activity," *Theoretical Issues in Ergonomic Science* (in production, 2011).

[4] A notion also observed by Russell Ackoff. See Russell L. Ackoff, "Transforming the Systems Movement," Opening Speech at the 3rd International Conference on Systems Thinking in Management (ICSTM 2004), Philadelphia, Pennsylvania, May 2004, URL: <http://www.acasa.upenn.edu/RLAConfPaper.pdf >, accessed 9 December 2010. Cited hereafter as Ackoff, "Transforming."

[5] Karl E. Weick, *Sensemaking in Organizations* (Thousand Oaks, CA: Sage Publications, Inc., 1995), and Brenda Dervin, "Sense-Making Methodology Site," URL: <http://communication.sbs.ohio-state.edu/sense-making/>, accessed 12 September 2007. Cited respectively hereafter as Weick, *Sensemaking*, and Dervin, "Sense-Making."

[6] Weick, *Sensemaking*, 2.

[7] Dervin, "Sense-Making."

[8] See Moore, *Sensemaking*.

[9] Ackoff Center Weblog, "Russell L. Ackoff, Management Consultant & Systems Thinker, 1919 -2009," 30 October 2009, URL: <http://ackoffcenter.blogs.com/ackoff_center_weblog/2009/10/russell-l-ackoff-management-consultant-systems-thinker-90.html>, accessed 9 December 2010.

[10] Ackoff, "Transforming."

[11] Ackoff, "Transforming."

[12] See the 9/11 Commission, *9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, DC, GPO, 2003), for a summary of the "failure" to prevent the tragedy of that day. Similar language was used regarding the Christmas 2009 attempted airline bombing. One could use the same kind of language to characterize the 1941 Japanese attack on Pearl Harbor and, for that matter, the failure of the Trojans to anticipate what was contained in that amazing horse which turned up outside their gates one day.

[13] Bruce Chew, conversation with the author, 2 June 2008.

[14] See, for instance, Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2007). Cited hereafter as Betts, *Enemies of Intelligence*.

[15] Perhaps, but given the intended audience a 2x4 might be needed… Planck observed, "A new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die, and a new generation grows up familiar with it." Max Planck, *Scientific Autobiography and Other Papers*, F. Glynor, trans. (New York, NY: Philosophical Library, 1949), 33-34. Cited in Charles Weiss, "Communicating Uncertainty in Intelligence and Other Professions," *International Journal of Intelligence and CounterIntelligence*, vol. 21, no. 1 (Spring 2008), 78-79.

[16] Thomas Kuhn, *The Structure of Scientific Revolutions* (Chicago, IL: University of Chicago Press, 1962), 10-42.

[17] This is a U.S. government-operated, Congressionally-chartered, and nationally accredited institution that offers Bachelor and Master of Science degrees in strategic intelligence for members of the U.S. Intelligence Community. Moore attended the institution during the 2001-02 academic year.

[18] Including Moore in a memorable class held less than a week after the attacks of 9/11 (2001).

[19] See the United States Office of Personnel Management, *Position Classification Standard for Intelligence Series*, GS-0132 TS-28, June 1960, and TS-27, April 1960, URL:<http://www.opm.gov/fedclass/html/gsseries.asp>, accessed 8 December 2010.

[20] For a fuller discussion see Moore, *Sensemaking*, especially chapters one and two.

[21] Mark Stefik, "The New Sensemakers: The Next Thing Beyond Search Is Sensemaking," *Innovation Pipeline* (15 October 2004), URL: <http://www.parc.com/research/ publications/files/5367.pdf>, accessed 9 December 2010.

[22] Moore, *Sensemaking*.

[23] See Gary Klein, Brian Moon, and Robert R. Hoffman, "Making Sense of Sensemaking 1: Alternative Perspectives," *IEEE Intelligent Systems*, vol. 21, no. 4 (July/August 2006), 71, 72; Peter Pirolli, *Information Foraging Theory: Adaptive Interaction with Information* (Oxford, UK: Oxford University Press, 2007); Peter Pirolli and Stuart Card, "The Sensemaking Process and Leverage Points for Analyst Technology as Identified Through Cognitive Task Analysis," paper presented at the 2005 International Conference on Intelligence Analysis, Vienna, Virginia, 2-6 May 2005, URL: <https://analysis.mitre.org/proceedings_agenda.htm#papers>, accessed 11 March 2009; David A. Schum, *Evidence and Inference for the Intelligence Analyst*, 2 volumes (Lanham, MD: University Press of America, 1987); Mark Stefik, "The New Sensemakers: The Next Thing Beyond Search Is Sensemaking, " *Innovation Pipeline* (15 October 2004), URL: <http://www.parc.com/research/publications/files/5367.pdf>, accessed 11 March 2009.

[24] Gary Klein, Jennifer K. Phillips, Erica L. Rall, and Deborah A. Peluso, "A Data/Frame Theory of Sensemaking," in Robert R. Hoffman, ed., *Expertise out of Context: Proceedings of the Sixth International Conference on Naturalistic Decision Making*, Boca Raton, FL: Taylor and Francis, 2007).

[25] Quoted in Ackoff, "Transforming."

[26] Gerald R. Nosich, *Learning to Think Things Through*, 3rd edition (Upper Saddle River, NJ: Pearson, 2009), 105.

[27] See Gregory F. Treverton, "Estimating Beyond the Cold War," *Defense Intelligence Journal* 3, no. 2 (Fall 1994), 5-20.

[28] Russell L. Ackoff, *The Art of Problem Solving* (New York, NY: Wiley & Sons, Inc., 1978), 6.
[29] Gregory F. Treverton, "Foreword," in David T. Moore, *Sensemaking: A Structure for an Intelligence Revolution* (Washington, DC: NDIC Press, 2011), v. Cited hereafter as Treverton, "Foreword."
[30] Treverton, "Foreword," v.
[31] Treverton, "Foreword," vi. See also Gregory F. Treverton, "Addressing Complexities in Homeland Security," in Loch Johnson, *The Oxford Handbook of National Security Intelligence* (Oxford, UK: Oxford University Press, 2010), 344. Treverton's use of the term is derived from David Snowden, "Complex Acts of Knowing: Paradox and Descriptive Self-Awareness," *Journal of Knowledge Management*, vol. 6, no. 2 (2002), 100-111; also available at: URL: <http://kwork.org/Resources/Snowden.pdf>, accessed 8 December 2010.
[32] See Horst W.J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences* 4 (1973), 155-169, cited hereafter as Rittel and Webber, "Dilemmas"; and Robert Horn, "Knowledge Mapping for Complex Social Messes," presentation to "Foundations in the Knowledge Economy" at the David and Lucile Packard Foundation, 16 July 2001, URL: <http://www.stanford.edu/~rhorn/a/recent/spchKnwldgPACKARD.pdf>, accessed 8 December 2010.
[33] Treverton, "Foreword," vi.
[34] This is one of the characteristics of a "wicked problem." See Rittel and Webber, "Dilemmas," 161.
[35] Ellen J. Langer, *Mindfulness* (Cambridge, MA: Da Capo Press, 1989), 27. Cited hereafter as Langer, *Mindfulness.*
[36] Langer, *Mindfulness*, 69.
[37] See Karl E. Weick and Kathleen M. Sutcliffe, *Managing the Unexpected: Resilient Performance in an Age of Uncertainty* (San Francisco, CA: Jossey-Bass, 2007).
[38] Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1949).
[39] Kendall, "Function," 551.
[40] Willmoore Kendall, "The Function of Intelligence," *World Politics*, vol. 1, No. 4 (July 1949), 549. Cited hereafter as Kendall, "Function."
[41] Unfortunately, we cannot go back in time and see if some other paradigm might have worked better. However, given a rising level of ignorance about many lesser known intelligence failures among younger intelligence personnel, a time may be coming when they can be resubjected to scrutiny using different paradigms. Those examining them will not know (except in a very general manner) what occurred.
[42] Sherman Kent, "A Crucial Estimate Revisited," *Studies in Intelligence*, vol. 8, no. 2 (1965).
[43] Paul Slovic, "Behavioral problems of adhering to a decision policy," paper presented at the Institute for Quantitative Research in Finance, Napa, CA, May 1973.
[44] Gary Klein, Karol G. Ross, Brian M. Moon, Devorah E. Klein, Robert R. Hoffman, and Erik Hollnagel, "Macrocognition," *IEEE Intelligence Systems*, vol. 18, no. 3 (May 2003), 82. Cited hereafter as Klein et alia, "Macrocognition."
[45] Klein et alia, Macrocognition," 81.
[46] Peter Schwartz and Doug Randall, "Ahead of the Curve," in Francis Fukuyama, ed., *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics* (Washington, DC: Brookings Institution Press, 2007), 97-98. Being systematic refers to clearly laying out the argument about why one believes certain futures are likely to the policymaking consumer.
[47] Klein and others, "Macrocognition," 82-83.
[48] Gary Zukav, *The Dancing Wu Li Masters: An Overview of the New Physics* (New York, NY: Harper Collins, 2001), 117.
[49] David T. Moore, Elizabeth J. Moore, William N. Reynolds, James Holden-Rhodes, and Marta S. Weber, "Making Sense of Non-State Actors: A Multimethod Case Study of a Wicked Problem," in David T. Moore, *Sensemaking: A Structure for an Intelligence Revolution* (Washington, DC: NDIC Press, 2011).
[50] Ackoff, "Transforming."
[51] Klein and others, "Data/Frame Theory," 119. See also Ulric Neisser, *Cognition and Reality: Principles and Implications of Cognitive Psychology* (San Francisco: Freeman, 1976).
[52] Klein and others, "Data/Frame Theory," 119.
[53] Klein and others, "Data/Frame Theory," 119. See also Ulric Neisser, *Cognition and Reality: Principles and Implications of Cognitive Psychology* (San Francisco: Freeman, 1976).
[54] Klein and others, "Data/Frame Theory," 119.
[55] Klein and others, "Data/Frame Theory," 119.
[56] Such cognitive shortcuts are sometimes referred to as mindsets and biases. We have elaborated elsewhere why we find such language dangerous. Nevertheless, we note that these arise from a confluence of cognitive limitations through which observations of reality are filtered. We also note that technological approaches reflect the respective underlying and underlying frames. Indeed, it exacerbates a false sense of confidence in selected frames because people (Americans at least) tend to unquestioningly accept the results from technology.
[57] Richards Heuer characterized this as "principles of perception." Minds are quickly made up, once formed, opinions are hard to change, and a great deal of contradictory data is needed to force such a change; most data are forced to fit the pre-existing frame. See Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999), 11-14. Cited hereafter as Heuer, *Psychology*.
[58] Heuer, *Psychology*, 14.
[59] See Moore, *Critical Thinking*, and Hoffman and others, "Critical Thinking."
[60] Klein and others, "Data/Frame Theory," 126.
[61] Rob Johnston identified over 160 so-called analytic methods being used by analysts in his research into how the Community creates intelligence. See Dr. Rob Johnson, *Analytic Culture in the U.S. Intelligence Community* (Washington ,DC: Central Intelligence Agency, Center for the Study of Intelligence, 2005), xviii. Many such methods have been collected and published. See, for instance, Richards J. Heuer and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Washington, DC: CQ Press, 2010). The list of techniques is likely much greater, for Johnston focused on what was being used in government intelligence and did not consider the domains of competitive intelligence. See also Craig S. Fleisher and Babette Bensoussan, *Strategic and Competitive Analysis: Methods and Techniques for Analyzing Business Competition* (Upper Saddle River, NJ: Pearson-Prentice Hall, 2002). Few of the methods in use in the Intelligence Community have been properly validated and, indeed, some have been shown to be of questionable validity. See, for instance, Brant A. Cheikes, Mark J. Brown, Paul E. Lehner, and Leonard Adelman, *Confirmation Bias in Complex Analyses*, Mitre Technical Report**,** MTR 04B0000017 (Bedford, MA: Mitre, 2004).

[62] National Security Agency, Suite 6158, 9800 Savage Road, Fort George G. Meade, MD 20755-6158.
[63] Institute for Human Machine Cognition, 40 South Alcaniz Street, Pensacola, FL 32502-6008.*on Naturalistic Decision Making*, Boca Raton, FL: Taylor and Francis, 2007).

David T. Moore is a senior intelligence professional and educator at the National Security Agency.[62] *He teaches critical thinking and structured techniques for intelligence sensemaking and his research focuses on developing multidisciplinary approaches to facilitate all aspects of intelligence sensemaking. His most recent posting was to the James Clapper School of Leadership and Professional Development at the National Geospatial-Intelligence Agency. He received a Master of Science of Strategic Intelligence from the National Defense Intelligence College in 2002. Correspondence should be directed to the author at david.t.moore@ugov.gov.*

Dr. Robert R. Hoffman is a senior research scientist at the Institute for Human-Machine Computing. He is recognized as one of the world leaders in the field of cognitive systems engineering and Human-Centered Computing.[63] *He is a Fellow of the Association for Psychological Science and a Fulbright Scholar. His current work involves the evaluation of knowledge management and performance measurement for macrocognitive work systems.*

The authors gratefully acknowledge the assistance of Gary Klein and Anthony Olcott in the preparation of this article.

Adapting U.S. Military Intelligence to Network Warfare

by Thomas F. Ranieri

INTRODUCTION

Everything has changed. The invention of the Internet and the electronic network, along with a thousand other technological and scientific advances, has fundamentally transformed the way that human society functions. Those nations which have adapted to technological progress, such as the United States, are the pinnacles of civilization, and enjoy more prosperity, efficiency, comfort, and power than the majority of the world. Just as civilian lives have been improved by technology, conventional military forces have also become more capable and deadly. Yet, as the U.S. experience in Afghanistan and Iraq has shown, there are people who can challenge such leviathans without drones, tanks, or any other cutting edge technology. The problems involved with fighting an insurgent or terrorist network indicate the shape of warfare to come. The strategies utilized by these groups are revolutionary.

One of the most vital steps to a new approach toward warfare must be a reformation of the U.S. military intelligence paradigm.

A new breed of warfare requires new strategies and tactics. One of the most vital steps to a new approach toward warfare must be a reformation of the U.S. military intelligence paradigm. Military intelligence must adopt a ground-level, decentralized approach, which emphasizes seamless integration into all military action and takes a full spectrum approach to intelligence gathering and dissemination.

THE PROBLEMS OF THE 21ST CENTURY

Fighting insurgencies has demonstrated the vulnerabilities of the U.S. armed forces, but it has also shown the direction in which war is moving. War is no longer merely about large, conventional armies maneuvering about a continental land space, clashing in epic battles. Rather, the process of total war, begun in the early 19th century, has reached its fulfillment. Not only the army—but the entire economic, political, civil, and military infrastructure of a nation—is subject to attack in what can only be described as full spectrum warfare:

> The ultimate goal of our military force is to accomplish the objectives directed by the National Command Authorities. For the joint force of the future, this goal will be achieved through full spectrum dominance – the ability of US forces, operating unilaterally or in combination with multinational and interagency partners, to defeat any adversary and control any situation across the full range of military operations.[1]

The technologies on which modern society is based—the Internet, global communications, satellites, and global positioning systems, to name just a few—are particularly vulnerable to the new total war.[2] This is because the inter-connectedness and globalization these technologies engender means that economic and political power are centralized in a few powerful states, and a centralized power structure is vulnerable to decentralized networks and guerrilla warfare.[3] There are benefits to centralization, such as increased control, harmony of interests, and unity of effort. Whether those benefits outweigh the liabilities of rigidity, sloth, and the potential disruption of the chain of command is another question entirely.

From a military perspective, these circumstances should be frightening. The Industrial Age, top-down, bureaucratic style of organizing and fighting wars, which was the hallmark of the U.S. military for the past hundred years,[4] is simply no longer effective in the Information Age. Archaic strategy is harmful to any military, but for the linchpin of the international order to have an outdated fighting force is death.

The monopoly on power that the American military enjoys has a major unintended consequence. The U.S. is so conventionally powerful that no one will fight it conventionally. As Max Boot puts it, "states will increasingly turn to unconventional strategies to blunt the impact of American power."[5] Insurgency, guerrilla

warfare, terror, cyber warfare, and political warfare are all asymmetrical responses to American military power.

A commonality among these responses is a reliance on decentralized networks to defeat large, centralized opponents by engaging them in every battlespace. Since total military defeat of the American military is impossible, adversaries attack on any front in which they can win, and refuse battle on those they cannot.[6] The decentralized network is absolutely essential to this strategy, because a network can have a node anywhere it needs without reference to space or national boundaries, and is versatile enough to perform any role that is required of it. Entire global networks can coordinate and attack through the use of cheap, instantaneous communications unencumbered by bureaucracy or hierarchy.[7] This makes them infinitely flexible, responsive, stealthy and, most of all, quick. Conversely, the American military, organized for large-scale combat, is constrained by a hidebound bureaucracy that is simply unable to compete.[8]

A networked strategy can be adopted by a nation-state's military as well, because it is simply a way of thinking and acting rather than a state of being.

Nevertheless, there is nothing to prevent the U.S. military from adopting appropriate principles of network warfare.[9] There is a correlation between these terrorist and insurgent groups and the use of a network strategy, but it is not exclusive to them. A networked strategy can be adopted by a nation-state's military as well, because it is simply a way of thinking and acting rather than a state of being. In many ways, nation-states are better suited to adopting this strategy, because of the resources and technology they can utilize which insurgent or terrorist networks cannot. It is the strength of the strategy, not its practitioners, that makes it so effective.

NETWORKS AND NETWARS

Though networks themselves are not new, they have been utilized in innovative new ways. A network is essentially a meta-grouping of organizations, interests groups, and individuals, called nodes, which are connected by an organizing or motivating principle—be it business or politics, terrorism or peace—and who are in communication with one another.[10] However, in the past, networks have been constrained by the limits of communication and technology; hence, their utility, especially for fighting wars, has also been limited.

The Internet has ushered in an age of cheap, instantaneous communications worldwide which is both anonymous and nearly impossible to trace. Now nodes can communicate with one another quickly, and organize and act toward a goal regardless of geographic realities. Entire networks, then, can be quickly called up to execute tasks across the globe in concert and be organized in such a way that their action has the greatest effect.

There are two characteristics of the archetypal network that are relevant to this discussion. The first is that a network communicates according to the circumstances and mission in which it finds itself. Certain nodes will communicate with others depending on the task set before them, but when that task is complete the communication will end:

> First, communication and coordination are not formally specified by horizontal and vertical reporting relationships, but rather emerge and change according to the task at hand. Similarly, relationships are often informal and marked by varying degrees of intensity, depending on the needs of the organization.[11]

The communication of a network is mission-oriented and effects based; it is completely focused. Inter-nodal contact for the transfer of intelligence and joint planning is not obstructed by service rivalry, stovepipes, or bureaucratic regulations.[12]

The second characteristic of the network is the breadth of contacts indirectly connected to the network through individual nodes. The network itself is connected by a shared belief or motivation, but the individual contacts of a node can be utilized even though they are not technically part of the network.

> Second, internal networks are usually complemented by linkages to individuals outside the organization, often spanning national boundaries. Like internal connections, external relationships are formed and wind down according to the life cycle of particular joint problems.[13]

A non-network node can be activated by network nodes that are connected to them, though the motivating principle will be coercion, money, or mere sentiment rather than shared ideology.

The informality of a network is a significant factor in its success. Individual nodes may have a strict hierarchy and discipline, but that does not reflect the organization of the network. Leaders of nodes can frankly discuss problems and solutions with less concern for status or career – they are already the head of a node.

> …[T]he principles of a networked organization [are] relative flatness, decentralization, and delegation of decision-making authority, and loose lateral ties among dispersed groups and individuals.[14]

The safety of their position means that they feel more secure in proposing and carrying out radical or unconventional tactics or strategies, independently if necessary. In a node, the innovators are the practitioners. Networks are more sensitive to problems, and new tactical and operational solutions can be tested and implemented swiftly, providing the network with immense flexibility.

The network is a new organizational strategy, along whose lines the spectrum of civil and "uncivil" society is organizing itself spontaneously. Civil society movements from around the world have begun utilizing the network strategy to great effect, just as terrorist and insurgencies have done.[15] The unique characteristics of the network have led warfare into a new era, with different rules, tactics, and strategies, termed[16] Fourth Generation Warfare.[17]

FOURTH GENERATION WARFARE

The United States has a global monopoly on force. For those groups that wish to oppose it. a new form of warfare had to be utilized. Fourth Generation Warfare was born as a result of this need. The modern insurgencies that the United States has been forced to fight in the 21st century have focused Western thinking about warfare and its trajectory. To remain capable of projecting power and to act as a stabilizing influence throughout the world, the United States must learn from the strategies of its enemies.

Fourth Generation Warfare finds its beginning in the Communist insurgency in China.[18] During this conflict, Mao Tse-tung wrote what can be considered the foundational document of fourth generation warfare, *On Guerrilla Warfare*. With Mao's strategy, the Communists defeated the Japanese and the Nationalists and conquered China. The book establishes two main distinguishing characteristics of Fourth Generation Warfare: (1) that all war is fought for political objectives, and therefore must always gear every action toward a political end; and (2) that actual fighting is only one tool among many to accomplish those goals.

The link between insurgent and Fourth Generation Warfare is that war is only one aspect of a political struggle:

> In the conventional war, military action, seconded by diplomacy, propaganda, and economic pressure, is generally the principal way to achieve the goal. Politics *as an instrument of war* tends to take a back seat and emerges again – as an instrument – when the fighting ends… The picture is different in the revolutionary war… the operations… are essentially of a political nature. In this case, consequently, political action remains foremost throughout the war.[19]

If the military is not directed by political aims, and integrated with other methods of war—political war, cyber warfare, information warfare, psychological warfare, to name a few—it does not stand a chance against an enemy that is so directed. This lesson will dictate both the nature of the war in the foreseeable future as well as the new intelligence requirements and paradigms necessary to support these new warfighters.

Success in Fourth Generation Warfare requires utilizing the entire spectrum of the tools of statecraft:

> These guerrilla operations must not be considered as an independent form of warfare. They are but one step in the total war, one aspect of the revolutionary struggle… We consider guerrilla operations as but one aspect of our total war or mass war because they, lacking the quality of independence, are of themselves incapable of providing a solution to the struggle.[20]

Netwar is focused on achieving a political objective, not a military one. As such, to use force where none is required is counter-productive to completing the political mission.

> Paraphrasing Clausewitz, we might say that "Insurgency is the pursuit of the policy of a party by any means available." It is not like an ordinary war – a "continuation of the policy by other means" – because an insurgency can start long before the insurgent resorts to the use of force.[21]

Militaries which follow Clausewitz's theory, that is to say, standard contemporary military forces and doctrine, are immediately at a disadvantage. Whereas the netwarrior or insurgent has an entire spectrum of means to accomplish objectives,[22] standard militaries only have one – force.

The full spectrum approach to warfare requires a shift of strategic thinking on the part of warfighters.

The full spectrum approach to warfare requires a shift of strategic thinking on the part of warfighters. Rather than emphasizing the destruction of enemy targets, the

netwarrior carries out action precisely calculated to bring about the strategic or tactical effect he desires.

> Strategically, 4GW [*sic*] attempts to directly change the minds of enemy policy makers. This change is not to be achieved through the traditional method of superiority on the battlefield… Their victories are accomplished through the superior use of all available networks to directly defeat the will of the enemy's leadership… In attempting to change the minds of key decision makers, antagonists will use a variety of tactical paths to get their message through to presidents, prime ministers, members of cabinets, legislators, and even voters.[23]

Both traditional and non-traditional means will be pursued to achieve the desired effect in Fourth Generation Warfare.

Full spectrum operations are amplified by the international media, and the ease of access to information.[24] Small events can have strategic consequences which affect the entire course of the war, because the media will amplify the event and instantaneously transmit it across the world.

> We come now to the other manner in which we fight and operate amongst the people in a wider sense: through the media. Television and the Internet in particular have brought conflict into the homes of the world – the homes of both leaders and electorates. Leaders are influenced by what they see and by their understanding of the mood of the audience, their electorate… We are conducting operations now as though we were on a stage…[25]

This circumstance makes information and political warfare much more potent, and works to the strength of Fourth Generation Warfare, namely, that tactical action can be translated into strategic effects. However, the downside to media amplification is that mistakes are even less affordable than they once were.

Fourth Generation Warfare is an evolution in the way men fight wars, and the U.S. military must evolve with it or risk being out-fought by the Third World.

To its credit, the U.S. military has recognized these dangers, and has been organically adapting to it. Warfare is a Darwinian affair, and those who do not adapt die. Fourth Generation Warfare is an evolution in the way men fight wars, and the U.S. military must evolve with it or risk being out-fought by the Third World.

EFFECTS-BASED OPERATIONS

Effects-based Operations is a theory of operational warfare and planning which is somewhat controversial. EBO incorporates Fourth Generation Warfare principles and adapts them to the unique circumstances of the U.S. Military. EBO is unique in that it concentrates on the political ends of warfare and uses full spectrum means to bring about the effects necessary to accomplish those ends.

Effects-based Operations and Netwar are complementary. Effects-based Operations seek to have all action, kinetic and non-kinetic, produce effects amenable to the political end of the conflict; Netwar essentially does the same thing on a different scale. The main difference is that Netwar uses small, interconnected, transnational nodes to accomplish objectives across the globe, while Effects-based Operations use military units and are concentrated in an Area of Operations. Despite this organizational difference, Effects-based Operations still fight in the same battlespace as does Netwar, and so it is the best chance for the United States to adapt to 21st century strategic innovations.

The switch from the traditional military mindset of defining an objective, delegating a task, and accomplishing it with little regard for the full spectrum of its effects will be difficult but necessary. That paradigm simply no longer fits the reality in which we find ourselves.

To fight and win future wars…will require reorganizing conventional militaries to emphasize such skills as cultural awareness, foreign language knowledge, information operations, civil affairs, and human intelligence.

Countering such threats [as Netwar] will require much more than simply buying increasingly advanced aircraft, tanks, and submarines. Such traditional weapons may be almost useless against adversaries clever enough to avoid presenting obvious targets for precision guided munitions. To fight and win future wars… will require reorganizing conventional militaries to emphasize such skills as cultural awareness, foreign language knowledge, information operations, civil affairs, and human intelligence. It will also require cutting away the bureaucratic fat to turn bloated industrial age hierarchies into lean information age networks capable of utilizing the full potential of high-tech weapons and highly trained soldiers.[26]

Effects-based Operations, especially if coupled with network-focused organizational reforms, is designed to be responsive and effective in the 21st century.

Traditional warfare separates the tactical, the operational, and the strategic levels of conflict,[27] so that there is a cognitive disconnect between them. As an intellectual exercise, this separation can be helpful in understanding different levels of action. However, it is also a contrivance, and obscures a fundamental truth of the battlefield: tactical action often translates to strategic effect.[28] In Fourth Generation Warfare, this truth has even greater importance, because media and instantaneous communication amplify the effect of tactical action to global scales:

> Media make it possible for a global audience to witness a small unit leader in action, capturing the effects of his decision in real time. These effects can be positive if they create opportunities and support the overall strategy, or they can be negative if they limit future opportunity or detract from the overall strategy.[29]

Effects-based Operations acknowledge this link between the strategic, operational, and tactical, and seek to determine behavior based on these factors.[30] By approaching conflict holistically, there is greater awareness of how to transform tactical action into strategic benefit.

Another way of looking at the overlapping relationship between the strategic and tactical level of conflict is to consider the link between political goals and local action. Political goals are the driving force behind strategy; they define the ends sought and the means to achieve them. Any action taken at any level which is not in accord with the political ends of an operation is by definition harmful. Conversely, any action taken which helps accomplish political goals is by definition helpful. Local or tactical action is therefore strategic insofar as strategic success is impossible without the conglomeration of many small acts adding up to large effects.

Global media have compounded this principle in two main ways. First, public relations are now important at all levels of action. Second, they it highlight the reality that every action taken has more than one effect, and that understanding those effects is absolutely the most important thing a warfighter can do:

> Just as one must validate the effectiveness of the initial attack – kinetic or non-kinetic – so must one register all subsequent reactions… It [Effects-based Operations] is a way of thinking that pushes planners to identify and exploit direct or cascading effects, links between the activities, persons, and infrastructure that can be affected and those activities, persons, and infrastructure that must be affected in order to achieve the stated political goals of the operation.[31]

Take, for example, the relatively prosaic task of delivering rice to a hungry village; it not only engenders goodwill in the local populace, but throughout the nation and the world if it is broadcast by the media. On the other hand, if the delivery of free rice bankrupts local businesses, then the net effect on public opinion is poor and is damaging to the economy and infrastructure.

Traditional approaches to warfare have ignored the importance of understanding the full range of effects an action may have because:

> The effect of one's actions on the enemy's political leadership or operational commander cannot be predicted accurately. Neither can one precisely anticipate the psychological effect on the enemy's will to fight or the attitude of the populace, particularly when the enemy's political and military culture is different from one's own… Intelligence simply cannot predict key aspects of the enemy's strategic behavior.[32]

Certainly, it is not easy to predict the full range of effects that an action may have; yet, terrorists and insurgents seem to have done so in the past.[33] At the very least, history has shown that actions primarily directed toward political objectives are cost-effective.

Unlike the current intelligence paradigm, which is focused on order of battle, technology, and targeting, the intelligence requirements for Fourth Generation Warfare are more comprehensive, including knowledge of localized conditions, as well as cultural and political intelligence.

This begs the question whether our inability to "predict key aspects of the enemy's strategic behavior"[34] is a result of national incompetence or, more likely, an outdated intelligence paradigm. Effects-based Operations are heavily dependent on accurate and timely intelligence in order properly to plan or anticipate effects. Unlike the current intelligence paradigm, which is focused on order of battle, technology, and targeting, the intelligence requirements for Fourth Generation Warfare are more comprehensive, including knowledge of localized conditions, as well as cultural and political intelligence.

The intelligence paradigm must evolve in order to remain pertinent and helpful to soldiers who must fight in a world of networks and Netwar.

WHY MILITARY INTELLIGENCE MUST CHANGE

A major problem with the current war in Afghanistan is that the commanders are not getting the intelligence needed to assist their decision-making. The Afghanistan conflict is Fourth Generational in nature. Traditional military intelligence, in its present paradigm, is unable to quickly provide the information needed to accomplish the mission:

> Eight years into the war in Afghanistan, the U.S. intelligence community is only marginally relevant to the overall strategy. Having focused the overwhelming majority of its collection efforts and analytical brainpower on insurgent groups, the vast intelligence apparatus is unable to answer fundamental questions about the environment in which U.S. and allied forces operate and the people they seek to persuade. Ignorant of local economics and landowners, hazy about who the powerbrokers are and how they might be influenced, incurious about the correlations between various development projects and the levels of cooperation among villagers, and disengaged from people in the best position to find answers – whether aid workers or Afghan soldiers – U.S. intelligence officers and analysts can do little but shrug in response to high level decision-makers seeking the knowledge, analysis, and information they need to wage a successful counterinsurgency.[35]

General Flynn clearly indicated the problem with the current intelligence system: it does not focus enough attention on the cultural and political realities that coexist on the battlespace. Yet, this is precisely what is needed to succeed in Fourth Generation Warfare.

It is particularly important to ensure that intelligence is correct and relevant in counterinsurgency because COIN warfare is an "intelligence driven endeavor."[36] The *Counterinsurgency Field Manual* defines the main purpose of intelligence in counterinsurgencies:

> Both insurgents and counter-insurgents require an effective intelligence capability to be successful… Intelligence in COIN is about people. U.S. forces must understand the people of the host nation, the insurgents, and the host nation government. Commanders and planners require insight into cultures, perceptions, values and beliefs, interests, and decision-making processes of individuals and groups… Insurgencies are local. They vary greatly in time and space. The insurgency one battalion faces will often be different than that faced by an adjacent battalion.[37]

The military intelligence apparatus has been failing to produce this information.[38]

Effects-based Operations require many improvements and innovations in intelligence in order to be effective, especially when used against Network-centric opponents:

> [Netwar] can become a problem in EBO if the supporting intelligence structure and protocols are ponderous or if the organizational focus has remained solely on databases for the large, traditionally-organized targets. Adversaries have also increased their use of IO, non-kinetic means, and other forms of coercion… The targeting quandary has thus become much broader than simply identifying the designated mean point of impact. In addition to databasing, effects-based intelligence must be capable of adaptive collection-and-analysis techniques to keep pace with increasingly complex engagement zones. Further, for this information to remain relevant it must be passed to the appropriate operators and acted upon before the enemy [reacts].[39]

Effects-based Operations must understand the culture and other local systems before manipulating them[40] and must have a mechanism to gauge the aftermath of actions taken to determine how effective or harmful they were.[41] They are also heavily reliant on the quick dissemination of intelligence. Approaches and tactics are added or adjusted to comply with intelligence feedback from past measured action. This type of intelligence makes Effects-based Operations dynamic and flexible. Insofar as Effect-based Operations are concerned, military intelligence has not been providing the proper support.

Military intelligence is not providing the information needed for warfare in the 21st century.

Military intelligence is not providing the information needed for warfare in the 21st century. It provides information that it is not what decision-makers require. As a result, our military is foundering.[42] The current military intelligence paradigm is outdated and a liability to U.S. armed forces.

HOW MILITARY INTELLIGENCE SHOULD CHANGE

The military intelligence paradigm must adapt to the overarching evolution of military operations in general. The needs of decision-makers have undergone a major shift, and to fight effectively they need local-level, cultural, political, and ideological intelligence in addition to intelligence about targeting, order of battle, and enemy organizational structure. This will require that intelligence change its method of collection, analysis, and dissemination. To adapt, military intelligence must change its institutional mindset and incorporate a network-centric model.

In a network, each node acts as both a sensor and an actor, and all intelligence produced from the node's activities quickly becomes shared knowledge throughout the entire network by utilizing information technologies.[43] This approach makes for well-informed and dynamic actors, who have both a situational awareness as well as an understanding of the global context for their actions.

Intelligence conducted according to a network-centric model, therefore, uses all soldiers as intelligence collectors. The *Counterinsurgency Field Manual* supports this method of intelligence collecting:

> The mosaic nature of insurgencies, coupled with the fact that all Soldiers and Marines are potential intelligence collectors, means that all echelons both produce and consume intelligence. This situation results in a bottom-up flow of intelligence.[44]

If one were to look at a squad as a close-knit network rather than simply a military unit, the implications become clearer. A soldier during his daily operations interacts with the people, gains an understanding of the local political power structures, and develops an appreciation for local culture, and then shares it as a part of his job. Each soldier in the squad multiplies the effect, both in collection and in dissemination of intelligence.[45] This is a tremendous source of information for intelligence officers and decision-makers who seek an understanding of the realities on the ground, as well as other platoons which face similar circumstances.

In addition to this, it would be necessary to increase the number of intelligence officers among small and active military units, who would act as focal points for the collection and dissemination of the intelligence gathered by the unit's members that day. By speaking to one another across the theater, they would learn from each other's mistakes, benefit from each other's information, and request information that they need from their peers. New enemy tactics would become known among friendly forces more quickly, which having been informed will more easily defeat them. Speaking in general, this sort of network would be more flexible and responsive, reacting to outside stimuli quickly and effectively across the entire theater of operations.

At present, military intelligence analysts have an eye only for their narrow subject matter and, whether it is helpful or not, produce intelligence on that subject alone.

> The tendency to overemphasize detailed information about the enemy at the expense of the political, economic, and cultural environment that supports it [is]… pronounced…[46]

The military must do more than improve the quality of its intelligence; it must fundamentally shift its organizational and institutional philosophy.

Analysis must expand its scope and concentrate more on a strategic, deep, and holistic view of the battlespace rather than narrow subject matter analysis. However, the military must do more than improve the quality of its intelligence; it must fundamentally shift its organizational and institutional philosophy.

Collective intelligence utilizes network principles to improve the quality and reliability of intelligence products. At present, our military intelligence analysts are too focused on secret and esoteric information, which they are either not allowed to share or are not interested in sharing, whether among themselves or with outside analysts.[47] The intelligence analyst network is mostly a closed circuit; hence, very little information is exchanged outside the intelligence community. To a certain extent this is helpful in keeping things secret. However, it also has the substantial downside of promoting a culture of irrelevance, where the intelligence produced is useless to the decision-maker.[48] Collective intelligence will address this issue by encouraging analysts to interact with experts outside of the intelligence community and to make use of open-source intelligence:

> The new paradigm, in contrast, will focus on "open source" information and reach out to a wide variety of experts who are non-intelligence professionals drawn from different sectors and often non-Americans… Indeed, it is an approach that attempts to synthesize knowledge found in various academic, business, and other private sectors with government expertise… the collaborative method is [for] scanning for interesting interconnections among issues, anomalies from what experts might normally expect to see, and other insights…[49]

By opening nodes of intelligence analysts to interaction with outside networks, they can benefit from outside knowledge and expertise. The network is thus expanded across an entire globe of experts and analysts, and collectively they can come to better conclusions than could a closed, smaller group with similar mindsets.

At present, the movement of information is based on a hierarchical system. Intelligence reporting and analysis is sent up the hierarchy, and then is sent down again to those whom the hierarchy deems needful. Unfortunately, this is both inefficient and unhelpful to decision-makers and operators alike:

> The soldier or development worker on the ground is usually the best informed about the environment and the enemy. Moving up through levels of hierarchy is normally a journey into greater degrees of cluelessness. This is why ground units, PRTs, and everyone close to the grassroots bear a double burden in a counterinsurgency; they are at once the most important consumers and suppliers of information.[50]

This method of intelligence dissemination is slow and it hurts the flexibility and situational awareness of those on the ground. Those to whom intelligence is disseminated must be expanded to include commanders across the spectrum of operations, from the platoon leader to the high-ranking decision-maker.

In short, the solution is that intelligence dissemination must become networked. Rather than simply sending up information to higher and higher levels of hierarchy and bureaucracy, intelligence officers should also network with each other, i.e., what is termed a semi-informal network. When adopted, this method has seen success in Afghanistan:

> The battalion intelligence officers refused to allow the absence of a data network to impede the flow of information. Each night, the deputy intelligence officer hosted what he called "fireside chats," during which each analyst radioed in from his remote position at a designated time and read aloud everything learned over the last 24 hours. Using this approach, daily reports incorporated a wide variety of sources… The deputy intelligence officer typed up a master report of everything called in by analysts and closed each chat session by providing them with an updated list of questions – called "intelligence requirements" – for the companies to attempt to answer.[51]

By sharing information and discussing problems, the network comes up with solutions to problems more quickly and is more responsive to the conditions on the ground than is a hierarchy. The network also benefits from having better informed and more effective operators and a holistic view of the battlespace.

Intelligence must change with the battlefield, and in so doing, change the way the military interacts with the battlefield.

The mindset of the intelligence officer must change. Rather than concentrating on information of purely military import, or of a narrow subject matter, intelligence should deal with the strategic or operational picture of a battlespace. It should recognize that cause and effect play out over all aspects of reality, and that, just as soldiers seek to engage in full spectrum warfare, intelligence officers must engage in full spectrum intelligence. The important type of intelligence in Fourth Generation Warfare is cultural and political, and focused on effects. In short, intelligence should orient itself toward acquiring the information necessary to accomplish political goals, so that planning, action, assessment, and adjustment are all part of a dynamic process.[52] Intelligence must change with the battlefield, and in so doing, change the way the military interacts with the battlefield.

A new intelligence paradigm is necessary to the success of U.S. armed forces in the field. These changes are strategic in nature - they are large steps which, if taken, could greatly improve the quality and relevance of the intelligence decision-makers have at their disposal.[53]

CONCLUSION

If the United States wishes to continue to ensure the safety and stability of the world, it must acknowledge and adapt to the changing social and military circumstances brought about by networks. The old method of engaging the world is incapable of addressing the threats and opportunities of a networked world. The greatest threat of the networked world is Fourth Generation Warfare, or Netwar. If the U.S. does not learn how to fight on these new terms, it will be unable to defeat its enemies.

Effects-based Operations is one of the first and most important moves toward dealing with the new way of war, but it has special intelligence requirements. Effects-based Warfare and Fourth Generation Warfare generally call for a new way to approach intelligence. A new paradigm which focuses on effects and cultural, political, and local intelligence to provide a holistic picture of the battlespace, and which adopts a network-centric strategy to make a responsive and flexible fighting force, will ensure success for the U.S. military in the 21st century.

Notes

[1] Joint Chiefs of Staff, *Joint Vision 2020* (Washington, DC: U.S. Government Printing Office, 2000), 6.
[2] John Arquilla, *Networks and Netwars* (Santa Monica, CA: Rand Corp., 2001), 1-15.
[3] John Arquilla, *Networks and Netwars* (Santa Monica, CA: Rand Corp., 2001), 1-2.
[4] Thomas Hammes, *The Sling and The Stone* (St. Paul, MN: Zenith Press, 2004), 192-193.
[5] Max Boot, "What the Past Teaches about the Future," *Joint Force Quarterly* 44, 2007, 115.
[6] An illustrative historical example of this approach can be found in the Cold War and the Soviet doctrine of "Correlation of Forces."
[7] Thomas Hammes, *The Sling and The Stone* (St. Paul, MN: Zenith Press, 2004), 195-197.
[8] Thomas Hammes, *The Sling and The Stone* (St. Paul, MN: Zenith Press, 2004), 193.
[9] John Arquilla, "The New Rules of War," *Foreign Policy*, March-April 2010, 62-63.
[10] John Arquilla, *Networks and Netwars* (Santa Monica, CA: Rand Corp., 2001), 10.
[11] John Arquilla, *Networks and Netwars* (Santa Monica, CA: Rand Corp., 2001), 31.
[12] Thomas Hammes, *The Sling and The Stone* (St. Paul, MN: Zenith Press, 2004), 192-193.
[13] John Arquilla, *Networks and Netwars* (Santa Monica, CA: Rand Corp., 2001), 31.
[14] John Arquilla, *Networks and Netwars* (Santa Monica, CA: Rand Corp., 2001), 33.
[15] John Arquilla, "The New Rules of War," *Foreign Policy*, March-April, 2010, 62-63.
[16] John Arquilla coins the term "netwar" in his writings but Hammes equates the two terms as meaning the same thing, insofar as behavior and characteristics of networks at war are concerned.
[17] Thomas Hammes, *The Sling and The Stone* (St. Paul, MN: Zenith Press, 2004), 5.
[18] Thomas Hammes, *The Sling and The Stone* (St. Paul, MN: Zenith Press, 2004), 3-4.
[19] David Galula, *Counterinsurgency Warfare*: *Theory and Practice* (Westport, CT: Praeger Security International, 2006), 4-5.
[20] Classic House Books, trans., Mao Tse-tung's *On Guerrilla Warfare* (Lexington, KY: Classic House Books, 2009), 2.
[21] David Galula, *Counterinsurgency Warfare*: *Theory and Practice* (Westport, CT: Praeger Security International, 2006), 1.
[22] It is important to note that Netwar does not in any way refute Clausewitz per se. However, his ideas must be understood in their proper context. Namely, they apply to that kinetic action which fits into a political schema but, conventionally understood, have limited utility in the other aspects of Fourth Generation Warfare.
[23] Thomas Hammes, *The Sling and The Stone* (St. Paul, MN: Zenith Press, 2004), 208-219.
[24] Ibid., 211.
[25] Rupert Smith, *The Utility of Force* (New York: First Vintage Books, 2008), 286.
[26] Max Boot, "What the Past Teaches about the Future," *Joint Force Quarterly* 44, 2007, 115.
[27] David Jordan, et al., *Understanding Modern Warfare* (New York: Cambridge University Press, 2008), 10.
[28] James E. Szepesy, "The Strategic Corporal and the Emerging Battlefield: The Nexus Between the USMC's Three Block War Concept and Network Centric Warfare" (MA thesis, Tufts University, 2005), http://www.carlisle.army.mil/DIME/documents/Szepesy[1].pdf (Accessed April 25, 2010).
[29] Ibid., 52-63.
[30] Steven Carey and Robyn Read, "Five Propositions Regarding Effects-based Operations," *Air and Space Journal* XX (2006).
[31] Ibid.
[32] Milan Vego, "Effects-based Operations: A Critique," *Joint Force Quarterly* 41, 2006, 53.
[33] A notable example of this occurred in Spain during its 2004 elections, when a well-timed terrorist attack derailed the course of the election in the terrorists' favor. Associated Press, "Socialists Declare Victory in Spanish Elections," *Fox News*, Monday, March 15, 2004, U.S. and World Section: http://www.foxnews.com/story/0,2933,114147,00.html (Accessed April 25, 2010).
[34] Milan Vego, "Effects-based Operations: A Critique," *Joint Force Quarterly* 41, 2006, 53.
[35] Michael T. Flynn, et al., "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Center for a New American Security, http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf (Accessed April 26, 2010).
[36] David H. Petraeus, et al., *The Counterinsurgency Field Manual* (Chicago, IL: University of Chicago Press, 2007), 79.
[37] Ibid., p. 80.
[38] Michael T. Flynn, et al., "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Center for a New American Security, http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf (Accessed April 26, 2010).
[39] Steven Carey and Robyn Read, "Five Propositions Regarding Effects-based Operations," *Air and Space Journal* XX (2006).
[40] J.P. Hunerwadel, "The Effects-Based Approach to Operations: Questions and Answers," *Air and Space Journal* XX (2006).
[41] Steven Carey and Robyn Read, "Five Propositions Regarding Effects-based Operations," *Air and Space Journal* XX (2006).
[42] Michael T. Flynn, et al., "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Center for a New American Security, http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf (Accessed April 26, 2010).
[43] "Thus information-age technologies are highly advantageous for a Netwar group whose constituents are geographically dispersed or carry out distinct but complementary activities. IT can be used to plan, coordinate, and execute operations. Using the Internet for communication can increase the speed of mobilization and allows for more dialogue between members, which enhances the organization's flexibility, since tactics can be adjusted more frequently." John Arquilla, *Networks and Netwars* (Santa Monica, CA: Rand Corp., 2001), 36.
[44] David H. Petraeus, et al., *The Counterinsurgency Field Manual* (Chicago, IL: University of Chicago Press, 2007), 79.
[45] Michael T. Flynn, et al., "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Center for a New American Security, http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf (Accessed April 26, 2010).
[46] Ibid.
[47] Ibid.
[48] Roger George, "Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm," Central Intelligence Agency, *Studies in Intelligence* (2007).

[49] Michael T. Flynn, et al., "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Center for a New American Security, http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf (Accessed April 26, 2010).
[50] Ibid.
[51] J.P. Hunerwadel, "The Effects-Based Approach to Operations: Questions and Answers" *Air and Space Journal* XX (2006).

Thomas F. Ranieri received his undergraduate degree in politics from the University of Dallas, where he concentrated his academic efforts in international affairs. He then matriculated at the Institute of World Politics in Washington, DC, from which he graduated with a master's degree in statecraft and national security affairs with a specialization in intelligence. During his time at the Institute, he focused his research on fourth generation warfare, or "netwar," and its implications for the field of intelligence. Mr. Ranieri has had a white paper published by the Diana Davis Spencer Foundation based on its roundtable discussion titled "Building Peace and Security in U.S.-China Relations," and an article posted in the Institute of World Politics online publication titled "The Militarization of Space: An Analysis of the Geopolitical Implications of Space Power in War." He is pursuing admission to an international affairs PhD program, and most recently has worked as an analyst at a small intelligence and security consulting firm.

Threats from Non-Traditional Actors:
Expanding and Transforming Intelligence to Address Transnational Issues

by Dr. Jennifer A. Davis

In December 2010, a man named Mohamed Bouazizi stood outside a government building in Sidi Bouzid, Tunisia, and set himself on fire in protest to his livelihood being confiscated by the provincial government and the governor's unwillingness to listen to his complaint.[1] His death struck a chord with many youths in Tunisia, who began using social networking sites such as Twitter and Facebook to organize protests against the government and coordinate rallies and marches. By January 14, 2011, President Zine El Abidin Ben Ali had been ousted from power, and from there the protests spread to Egypt, Libya, Syria, Yemen, Jordan, and throughout much of the Arab world. A month later, on February 11, 2011, President Hosni Mubarak announced that he would step down as the leader of Egypt after ruling for 30 years in the wake of widespread protests throughout the country, again largely coordinated, fostered, and managed through extensive use of social networking sites.[2] As of May 2011, protests continue throughout the Arab world and other dictators are struggling to maintain their holds on power in their countries as these protests spread.

In the modern era, threats come from many directions rather than just the traditional threats of armed rebellions or foreign military forces.

Until 2011, it is unlikely that any of these leaders – Ben Ali, Mubarak, Qaddafi, al-Assad, Saleh, or others – ever considered social networking sites, or even the use of the Internet, to be a real security threat to their regime. Yet the coordination of protests through the use of the cyber realm and its social networking sites has led to the resignation of two leaders so far, with others still in the balance. As one Egyptian activist succinctly tweeted during the protests in Egypt, "We use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world."[3] The recent U.S. experience with WikiLeaks also highlights the impact that non-state actors can have upon security and intelligence. The lesson which can be observed in the above example is that, in the modern era, threats come from many directions rather than just the traditional threats of armed rebellions or foreign military forces. While in this case the Arab Spring may provide positive steps for democracy in the Arab world, it also highlights how rapidly these new, transnational movements can impact state power and governance. In this case, these efforts were organized by opposition movements seeking more accountability and transparency from their governments, but it could just have easily occurred at the hands of less benign non-state actors seeking to oust their governments for more hardline, extremist parties as well.

Transnational threats are an increasing area of concern for U.S. intelligence and security professionals. While the traditional security paradigm has consisted of state-on-state interactions and conventional security threats such as nuclear proliferation, military strength and capabilities, or insurgencies, the realm of transnational threats has often been overlooked by intelligence analysts or relegated to issues considered human security rather than U.S. security. This paradigm worked remarkably well during the Cold War era, but began breaking down at the close of the last century and the beginning of the 21st century. In the modern era, threats come from many different types of actors – traditional states and governments still, but also non-state actors such as drug trafficking organizations and gangs, super-empowered individuals through the use of Internet programs such as Twitter and Facebook, and even through the spread of disease or viruses and cyber attacks waged in a very non-traditional battle space. In order to successfully adapt to a rapidly evolving environment, the Intelligence Community needs to include some of these non-traditional, transnational threats in its collection portfolio to be able to successfully meet and counter the rising security threats found outside of the traditional security context.

IDENTIFYING NEW THREATS

Transnational threats are not necessarily new, but the rapid speed of communication and travel, and the proliferation of new and evolving technologies, combine to make them especially relevant in the 21st century. In the most basic sense, a transnational threat is

any threat to security that crosses national borders. As most agencies use the term, it also includes the presence or role of non-state actors or elements; in practice, transnational threats include specific issues such as the threats posed by small arms trafficking, drug trafficking organizations, organized crime groups, human trafficking, the spread of diseases, and cyber threats such as bots, viruses, and virtual attacks on infrastructure or government agencies. This article will briefly examine each of these in turn, and then offer recommendations on how the Intelligence Community can adapt to better address these going forward.

SMALL ARMS TRAFFICKING

Small arms smuggling and proliferation is an incredibly lucrative trade for those actors engaged in the sale or smuggling of small arms, and the weapons themselves have a major role in threats to the state as well as to civilians. For example, in January 2010 a small group of narco-terrorists armed with assault rifles killed 16 teenagers and their families attending a birthday party in Ciudad Juarez, Mexico, on the U.S. border. A little over a year prior, in November 2008, two dozen terrorists belonging to Lashkar-e-Tayyiba killed nearly 200 people in Mumbai, India, and wounded an additional 350 civilians. They used basic small arms in their attack, composed of AK-47 rifles, 9mm pistols, and hand grenades.[4] Estimates suggest that as many as 875 million small arms are currently in circulation worldwide, only a third of which are in the hands of legally-constituted security forces. In Yemen alone, estimates state that there are as many as three small arms per person. Small arms are straightforward to use, easy to move or conceal, and often durable in harsh climates, allowing them to be moved across state lines and distributed among non-state actors with relative ease.

Estimates suggest that as many as 875 million small arms are currently in circulation worldwide, only a third of which are in the hands of legally-constituted security forces.

Small arms trafficking presents a direct and immediate threat to the U.S. on the U.S.-Mexico border. One of the most popular and frequent types of arms trafficking between the U.S. and Mexico is the *hormiga*, or ant, run, so called because the process is similar to ants carrying food back and forth to their hive. In a *hormiga* run, individuals traverse the U.S.-Mexico border in frequent trips carrying only one to three guns at a time. A legally eligible or "straw" purchaser buys a few weapons (often cheap .22- and .25-caliber pistols,"38 specials," and 9mm pistols) from gun stores in El Paso and other U.S. border towns and hands the mover to the trafficker, who sneaks him or her across the border, generally either on foot or in the trunk of a car.[5] These trips are repeated hundreds of time each year by different smugglers, making multiple trips to gun stores along the U.S.-Mexico border and selling the arms on the grey and black markets. Other forms of small arms trafficking occur when corrupt officials, or gangs and drug traffickers, sell or steal arms from military and police caches from countries such as Guatemala and El Salvador. These can include grenades, assault rifles, pistols, and other forms of small arms. In at least one episode, grenades seized from a military storage facility in Guatemala were used in an attack on the U.S. Consulate in Mexico.[6]

As this example shows, small arms trafficking can—and does—directly impact U.S. interests and security, and should serve to highlight the need for the Intelligence Community to track and monitor the movement of small arms on the grey and black markets. While there are some efforts in place within the Intelligence Community to track the movement of small arms and number of arms on the black market, these groups are often understaffed and unable to fully keep up with the rapid movement and flow of small arms sales around the world. At the very least, the Intelligence Community should continue to examine and track the role that small arms play in terrorism, insurgencies, and organized crime in order to best develop strategies in countering these actors.

DRUG TRAFFICKING

Drug trafficking is a continuing transnational issue in the intelligence and security communities, affecting the Americas, Asia, and Europe as well as spreading throughout Africa. While the drug trafficking routes throughout the Caribbean Basin have been well documented in intelligence studies, newer routes from South America to West Africa and up into Europe are becoming more and more popular as a means of moving illicit drugs.

Shipments of cocaine in particular originate in South America, and then are transferred by ship or aircraft to various countries in West Africa. From there, the drug shipments are broken down into smaller parcels and sent to Europe, in particular Spain and the United Kingdom, through a variety of means including commercial flights via luggage, clothing, or the bodies of couriers, as well as ships, smaller boats, and private air. Distribution is being controlled by criminal groups and drug trafficking organizations based in either West Africa or South

America.[7] Drug seizures are growing dramatically, with at least 46 tons of cocaine seized en route to Europe via West Africa since 2005. Prior to this period, all drug seizures throughout the entire continent of Africa combined rarely equaled one metric ton per year.

It appears that most cocaine entering Africa from South America makes landfall around one of two hubs, centered on Guinea-Bissau in the north and Ghana in the south. According to a 2008 report for the United Nations Office on Drugs and Crime, the couriers feeding these two markets show some clear patterns. Over 80% of the cocaine seized destined for Spain was taken from nationals of Nigeria, Guinea-Bissau, Mali, and Cape Verde. Two-thirds of the Nigerians embarked from Guinea or Mali. The market in the United Kingdom is even more concentrated among a few groups, with 75% of the couriers detected being Nigerian or British nationals. Over 60% of the Nigerians detected embarked from Nigeria, the single largest origin-destination pairing.[8] Additionally, there is increasing evidence that heroin is being trafficked from Afghanistan to Pakistan, through Kenya or Tanzania, and then to Europe in addition to the more traditional land-based routes.

Narcotics is still the most profitable illegal trade in the world, generating billions of dollars per year in revenue for its participants and helping to fund other illegal activities such as human trafficking, arms smuggling, and other black market activities.

As drug trafficking spreads from its traditional corridors in Asia and Latin America to newer, emerging routes in West and East Africa, the Intelligence Community needs to remain focused on the risks to security and stability through the proliferation of the narcotics trade and the profits generated for drug trafficking organizations and organized crime groups. Narcotics is still the most profitable illegal trade in the world, generating billions of dollars per year in revenue for its participants and helping to fund other illegal activities such as human trafficking, arms smuggling, and other black market activities.

HUMAN TRAFFICKING

Human trafficking and smuggling is one of the most lucrative black market activities at present, generating billions of dollars per year for organized crime syndicates and other actors. Human trafficking is currently tied with the small arms trade as the second most lucrative criminal activity after the narcotics trade. The United Nations estimates that around 2.5 million persons are trafficked annually, from 127 countries around the world.[9] International Labor Organization estimates state that the illicit profits produced by trafficked forced laborers are around $32 billion annually.[10]

Human smuggling is when a person is smuggled between one country and another and then released as an alien in the new country, whereas human trafficking involves a person being taken into captivity and used for labor against his or her will.

Human smuggling is when a person is smuggled between one country and another and then released as an alien in the new country, whereas human trafficking involves a person being taken into captivity and used for labor against his or her will. The *Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children*, more commonly known as the Palermo Protocol, defines human trafficking as:

> "the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs."[11]

Often, individuals start out as smuggled aliens but then become trafficked if they are not released.

A common misconception about human trafficking is that the majority of its victims are used in the sex trade; in fact, less than half of the victims annually are part of this trade though it varies by region. According to ILO statistics, of the estimated 9.5 million victims of forced labor in Asia, less than 10% of those are part of the sex trade.[12] Forced labor can include everything from factory workers, domestic laborers, agricultural forced labor, and construction workers to those employed in the sex trade.

The intelligence issues presented from human smuggling and trafficking take multiple forms. First of all, it is important that intelligence analysts and collectors broaden

their consideration of human trafficking and smuggling from strictly a human rights or human security concern to an intelligence issue as well. For example, trafficked victims can bring with them infectious diseases from their country of origin which proliferate rapidly within the close confines or poor sanitary conditions to which many forced laborers are subjected. Secondly, for those participating in the sex trade with trafficked persons, individuals are often reluctant to declare their whereabouts or activities to immigration or customs agents, again creating the risk of the spread of disease. In one specific instance in 2009, a businessman from Canada had flown to Thailand and engaged in multiple encounters with trafficked girls; during this time the businessman was exposed to H1N1 but concealed his condition from customs officials due to the nature of how he came into contact with the virus. Instead, an entire plane full of passengers was exposed to H1N1 for hours during the trans-Atlantic flight, and while in this case the virus was successfully contained it could easily have led to a significant outbreak.

Security concerns also stem from the tide of human smuggling as well. "Coyotes," the nickname for those engaged in human smuggling through Mexico, are working more and more with drug trafficking organizations such as Los Zetas, the Gulf Cartel, and other groups to bring illegal aliens into the U.S. In a few reported cases, Hezbollah agents have sought meetings with human smugglers in the Central American corridor, presumably to explore the options for having agents brought into the U.S. outside of legal customs channels. The Iran-backed Lebanese group has long been involved in narcotics and human trafficking in South America's Tri-Border Region of Paraguay, Argentina, and Brazil. Increasingly, however, it is relying on Mexican narcotics syndicates that control access to transit routes into the U.S.[13] Other terrorist groups are certain to follow, seeking transit from the Tri-Border Region of South America through Central America and into the U.S. through well-established human smuggling routes and channels. Human smuggling and trafficking are much more than a human rights issue; due to the potential for terrorist agents to use them as a means of illegally entering the U.S., the revenues generated for organized crime and drug trafficking organizations, and the risk of pandemics or spread of disease from individuals engaging in sex tourism abroad, human trafficking and smuggling are a rapidly evolving and growing transnational threat for intelligence analysts to investigate.

CYBER THREATS

In 2007 Estonia suffered one of the worst cyber attacks in history when a series of distributed denial of service type attacks were conducted against a number of Estonian websites, ranging from single individuals using various low-tech methods like ping floods to expensive rentals of botnets usually used for spam distribution. The attack came shortly after Estonia's removal of the Bronze Soldier Soviet war memorial in central Tallinn, leading many experts to look to Russia as the source of these cyber attacks. The crisis unleashed a wave of so-called DDoS, or Distributed Denial of Service, attacks, where websites are suddenly swamped by tens of thousands of visits, jamming and disabling them by overcrowding the bandwidths for the servers running the sites.[14] Sites affected included nearly all of the ministry offices of Estonia, the Estonian Presidency and Parliament websites, three of the country's six largest news organizations, and at least two national banks. Russia officially denied responsibility for these attacks, claiming the perpetrators were individuals acting on behalf of Russian nationalism and pride rather than any directed state attack.

A second cyber attack occurred a year later, in 2008 against Georgia during its conflict with Russia over South Ossetia and Abkhazia. Researchers at Shadowserver, a volunteer group that tracks malicious network activity, reported that the website of the Georgian President, Mikheil Saakashvili, had been rendered inoperable for 24 hours by multiple DDoS attacks. In addition to the DDoS attacks, some researchers said there was evidence of redirection of Internet traffic through Russian telecommunications firms as well as some Russian organized crime groups.[15] Some of the cyber attacks took down the websites for the Georgian Parliament and Georgian Ministry of Foreign Affairs, replacing them with propaganda and images comparing Georgian President Mikheil Saakashvili to Adolf Hitler.[16]

A more recent attack, known as Stuxnet, was discovered in 2010. Stuxnet operated much more strategically than the above attacks, singling out very specific computers that met certain configuration requirements. Stuxnet attacked Windows-based systems using an unprecedented number of zero-day exploits, or computer application vulnerabilities that have not yet been discovered, along with a CPLINK vulnerability and a vulnerability used by the Conficker worm. According to Symantec, Stuxnet was the first worm designed to actually reprogram industrial systems rather than simply spy on them or collect data from them.[17] Once installed on a PC, Stuxnet uses Siemens' default passwords to seek out and try to gain access to systems that run the WinCC and PCS 7 programs that are used to manage large-scale industrial systems on factory floors and in military installations and chemical and power plants.[18] The largest number of computers attacked by Stuxnet were located in Iran, with nearly 60% of Iranian computers infected.[19] The origin of Stuxnet is not known, but most

researchers believe it was by a highly capable and advanced organization or government, based on the skill required and advanced capabilities of the virus, rather than a group of individual hackers.

The United States is actively working to improve its cyber capabilities, such as the launch of U.S. Cyber Command at Fort Meade, Maryland, in 2009.

The use of cyber attacks is a rapidly evolving, and potentially significant, transnational issue that could significantly impact the way future conflicts are fought. Traditionally, security and intelligence efforts have focused on physical threats, such as the size of militaries, order of battle, or placement of strategic military capabilities such as bases or weapons facilities. In future conflicts, it is increasingly likely that at least some of the fights will be waged in the cyber realm, as adversaries seek to infect military and civilian computer systems with viruses, even potentially taking electrical or transportation facilities offline through DDoS attacks or viruses such as Stuxnet.

The United States is actively working to improve its cyber capabilities, such as the launch of U.S. Cyber Command, or USCYBERCOM, at Fort Meade, Maryland, in 2009. As technologies continue to evolve and other actors—both state and non-state groups—improve their own cyber capabilities, the U.S. Intelligence Community will need to continue focusing efforts on tracking and improving its cyber capabilities in order to stay on top of evolving cyber trends and prevent attacks on U.S. computer systems and other assets.

THE WAY AHEAD

Traditional security studies focus on the state's ability to defend itself from external threats. Too often, however, intelligence professionals have taken a narrow definition of security studies in their approach, identifying the sources of threats as other state actors and limiting the conception of the threats themselves to such activities as weapons proliferation and arms races, acquisition of weapons of mass destruction, or troop movements along strategic borders. However, in the rapidly evolving global environment of the modern era, threats can arise from any number of non-state actors as

well as governments: terrorist groups, organized crime syndicates, drug trafficking organizations and narco-terrorists, black market entrepreneurs such as Viktor Bout, and cyber "hacktivists." Other states and governments are no longer the sole entities able to mount a cohesive, significant security threat to the United States.

In order to meet these evolving, transnational threats, the Intelligence Community needs to leverage its assets to foster more cooperation and information sharing across these transnational issue areas. There is a good deal of cooperation between agencies at present; since so many of the transnational threats cross domestic and international boundaries, groups such as the Federal Bureau of Investigation, Customs and Border Protection (under the Department of Homeland Security), and the Drug Enforcement Administration collaborate and work closely with the Department of State, the Defense Intelligence Agency, and the Central Intelligence Agency to assist in the production of timely intelligence for the nation's leaders. Still, the establishment of more interagency task forces on key issue areas such as those discussed above, along with improved transparency among subject matter experts within these realms, will go a long way toward helping to improve the Intelligence Community's knowledge and ability to respond to these transnational threats.

Notes

[1] Al Jazeera, "How Tunisia's Revolution Began," accessed on April 27, 2010. Available at http://english.aljazeera.net/indepth/features/2011/01/201112612181598548 3.html.
[2] BBC, "Egypt's Mubarak Resigns as Leader," February 11, 2011. Available at http://www.bbc.co.uk/news/world-middle-east-12434532.
[3] Phillip N. Howard, "The Cascading Effects of the Arab Spring," *Miller-McCune*, February 23, 2011. Available at http://www.miller-mccune.com/politics/the-cascading-effects-of-the-arab-spring-28575/.
[4] Rachel Stohl and E.J. Hogendoorn, "Stopping the Destructive Spread of Small Arms," March 10, 2010.
[5] Lora Lumpe, "The U.S. Arms Both Sides of Mexico's Drug War," *Covert Action Quarterly*, Summer 1997, Vol. 61, 39-46.
[6] Nick Valencia, "Grenades explode near U.S. consulate in Mexico," CNN, October 2, 2010.
[7] Thibault Le Pichon, *Drug Trafficking as a Security Threat in West Africa*, United Nations, UN Office on Drugs and Crime, 2008.
[8] *Ibid*, p. 3.
[9] "UN backed container exhibit spotlights plight of sex trafficking victims," United Nations News Center, http://www.un.org/apps/news/story.asp?NewsID=25524&Cr=trafficking&Crl, accessed May 13, 2011.
[10] David Feingold, "Human Trafficking," *Foreign Policy*, No. 250, 2005, pp. 26-30.
[11] United Nations, *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime*, A/55/383, New York, November 15, 2000.
[12] International Labor Office, *A Global Alliance Against Forced Labor*, Geneva, 2005.
[13] Sara Carter, "Hezbollah uses Mexican drug routes into U.S.," *The Washington Times*, March 27, 2009.
[14] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian*, May 17, 2007.
[15] John Markoff, "Before the gunfire, cyber attacks," *The New York Times*, August 12, 2008.
[16] Travis Wentworth, "You've Got Malice: Russian nationalists waged a cyber war against Georgia. Fighting back is virtually impossible," *Newsweek*, August 12, 2008.
[17] Robert McMillan, "Siemens: Stuxnet worm hit industrial systems," *Computer World*, September 14, 2010.
[18] *Ibid.*
[19] Symantec Corporation, "W32.Stuxnet," 17 September 2010.

Jennifer A. Davis is a senior faculty member at the National Defense Intelligence College, specializing in globalization and transnational threat issues. She received her PhD degree in 2010 from George Washington University, focusing her research on child soldiering and international criminal law. She also conducts research on organized crime, human trafficking, and ethnic conflict as well as the development and progress of the International Criminal Court. Dr. Davis can be reached for more information at jennifer.davis@dodiis.mil.

Forming a Definitional Framework for "Intelligence"

by Lt Col (USAF, Ret) Milton Diaz

OVERVIEW

The Intelligence Community does not possess a formal theory by which to adapt, plan, and manage its limited resources. However, experts believe developing a theory will not be possible without first proposing a theoretical definition – a contentious topic in itself. Hypothesizing that a definition can be derived from diverse opinions, the author employees a social science field research technique, Q-methodology, to distill subjective arguments regarding "intelligence" to those elements necessary for distinguishing national intelligence from other disciplines. The author concludes the study by proposing a general, lexical definition and more precise theoretical definition for intelligence. Lacking the rigor necessary by which to define intelligence, this work, nonetheless, demonstrates an approach that resolves underlying, often emotionally charged arguments regarding what defines intelligence. Although dealing with opinions, Q-methodology provides a repeatable method of analyzing subjectivity and deriving defendable conclusions. This study also demonstrates Q-methodology's applicability to other emotion-laden debates such as that which took place concerning Iraq's alleged possession of weapons of mass destruction.

INTELLIGENCE THEORY: THE NEED FOR A DEFINITION

Since before the U.S. Intelligence Community's inception and for its foreseeable future the single most influential driver for change will be its failures. In each previous case – for example, the Japanese attack on Pearl Harbor, the Chinese intervention during the Korean War, the intensity of the Tet offensive, the 9/11 terrorists attacks on New York City and the Pentagon, and the flawed assessment regarding Iraqi weapons of mass destruction – the United States addressed its failure by enacting major organizational changes in its intelligence structure. Arguably, each shake-up set the stage for subsequent intelligence breakdowns by putting in place a static solution to the problems causing the last failure. Hence, the need for a guiding theory for intelligence – resting on a unifying definition of "intelligence" – by which government leadership might proactively address emerging threats through reasoned adaptation of its intelligence structure rather than principally relying on the study of past failures.

The IC has yet to develop a single, formal, and unifying theory or a theoretical definition of "intelligence."

In the sixty-plus years since the IC officially came into existence shortly after World War II, it has yet to develop a single, formal, and unifying theory or a theoretical definition of "intelligence." During this period, while many authors and organizations ventured to define intelligence, none of their proposals received universal acceptance. Even disciples of Sherman Kent – whose seminal and influential 1949 text, *Strategic Intelligence*, introduced "intelligence" to politicians, practitioners, and the general public as positive knowledge about foreign states, as a physical organization, and as an activity – alter Kent's treatises to suit their purpose.[1]

The IC's organizational challenge stems from a glut of theories rather than lack thereof. In *Intelligence Theory: Key Questions and Debates*, Peter Gill and his co-authors present theories from eleven intelligence experts. While each author posits a well-reasoned theory and corresponding definition, each differs in form and function. In the book's concluding chapter, Gill blends choice aspects from the preceding chapters into a theory of his own; however, his suggestion remains subjective. Noted British intelligence expert Phillip H.J. Davies wonders if an intelligence theory is necessary. Davies speculates that, until American departments and intelligence agencies stop bickering among themselves, "no amount of effort bent to finding new ways to think about intelligence, no revolution in intelligence theory or anything else will make any difference at all."[2] Although leery of intelligence theories, in effect, Davies suggests yet another theory. He hypothesizes that intelligence develops best when left to its

natural devices – organized common sense – in a collegial environment. Nevertheless, is Davies' concept superior to any of the theories he critiques? How does leadership select between theories and why is one superior to another?

Experts believe the key to developing an intelligence theory lies in first agreeing upon a theoretical definition of the term "intelligence."

Experts believe the key to developing an intelligence theory lies in first agreeing upon a theoretical definition of the term "intelligence." Historian Michael Warner argues that developing an intelligence theory without a sound theoretical definition providing its intellectual framework is a fruitless endeavor.[3] Gill concurs: "If we cannot agree on what we are discussing, then we shall struggle to generate understanding and explanation in an important field of political and social activity..."[4] Yet, for each theory, there exists a corresponding and subjective definition of "intelligence." Again, the question is how to select between these definitions.

Fortunately, a social science technique, Q-methodology, offers a mathematical means by which to probe and elucidate the subjectivity surrounding controversial subjects – in this case, the definition of intelligence. A disciplined approach, the Q-method consists of three phases, namely developing a set of survey statements, called the Q-sample; administering the surveys to intelligence officers, theorists, and consumers; and interviewing survey participants regarding their responses.

This article describes the field research and conclusions from which the author derived both a lexical definition for general intelligence and the limiting factors which narrow the lexical definition to the more precise region of a theoretical definition for intelligence.[5] In this study, the author theorizes that the many intelligence definitions carry some universal and obtainable truths. Employing the Q-methodology field research technique, the author extracts the logical elements from which individuals develop their subjective definitions of intelligence. He then hypothesizes that combining the logical basis for existing thinking regarding the meaning of intelligence will produce a framework – the essential elements – for a definition of intelligence.

The result of this study, a theoretical definition, could form the anchor for a formal theory – a testable model – by which intelligence agency and government leadership can grasp the complex intelligence system. Although time and resources limited the conclusiveness of the resulting definition, the study demonstrates Q-methodology's potential utility as a tool to derive a theoretical definition or tackle similarly subjective issues. Once achieving such a definition and corresponding theory, the IC will possess the means to test strategies, understand consequences, or guide decisions prior to initiating strategic changes to its structure, objectives, or methods.

THE RESEARCH METHODOLOGY

This study required the author to dissect conflicting arguments regarding "intelligence" and how the IC should operate. Intelligence officers have deeply held convictions based on training, experience, and reason regarding their individual definitions of intelligence. Often, their definitions are diametrically opposed with seemingly insurmountable obstacles. The topic of secrecy is one such example. Some intelligence officers say that the IC's contribution to decision-makers – "value added" – stems from reports and analysis of competitors' innermost secrets; otherwise, the news media could perform the IC's function. Other experts say that the IC's over-emphasis on secret materials leads to critical lapses that could be avoided had non-secrets or "open source" information carried similar credibility. While both arguments have merit, they appear incompatible. By using the Q-methodology, the researcher isolated subjective arguments regarding secrecy and other aspects of intelligence posited by study participants. The disciplined methodology consists of three phases, namely developing a set of survey statements, called the Q-sample; administering the survey to intelligence officers, theorists, and consumers; and interviewing survey participants regarding their responses. From the resulting mosaic of subjective opinion, the author derived a unifying definition which resolved contentious issues through criteria also attained during the field research.

PHASE I: DEVELOPING THE Q-SAMPLE

In the first phase, the author sought an expansive – though not exhaustive – set of published literature regarding intelligence through which to derive 62 declarative statements, the Q-sample. From definitions, theories, and stories of various intelligence authorities, academicians, and other theorists, Q-sample statements were written to assert an aspect of "intelligence" in a manner that reduced subtlety and provoked agreement or disagreement from the survey participants. Table 1 lists sources which inspired many of the Q-sample statements. The author derived other assertions from the comments and suggestions of intelligence analysts, peer reviewers, and academic advisors.

1. Sherman Kent. *Strategic Intelligence for American World Policy* (1949).
2. Lyman Kirkpatrick, Jr. *The U.S. Intelligence Community: Foreign Policy and Domestic Activities* (1973).
3. Mark M. Lowenthal. *Intelligence: From Secrets to Policy* (2006).
4. Loch K. Johnson. *Secret Agencies: U.S. Intelligence in a Hostile World* (1996).
5. David Kahn. "A Historical Theory of Intelligence." *Intelligence and National Security*, 16 (Autumn 2001).
6. Ameringer, Charles D. *U.S. Foreign Intelligence: The Secret Side of American History* (1990).
7. Adam N. Shulsky and Gary J. Schmitt. *Silent Warfare: Understanding the World of Intelligence* (1991).
8. Christopher M. Andrew. *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush* (1995).
9. Colonel Michael Dewar, British Army. *The Art of Deception in Warfare* (1989).
10. Tyler Drumheller and Elaine Monaghan. *On the Brink: An Insider's Account of How the White House Compromised American Intelligence* (2006).
11. Carl O. Schuster, Commander, USN. *Weather War*.
12. Editors Roger Z. George and James B. Bruce. *Analyzing Intelligence: Origins, Obstacles, and Innovations* (2008).
13. Editors Peter Gill, Stephen Marrin, and Mark Phythian. *Intelligence Theory: Key Questions and Debates* (2008).
14. Henry L. Stimson and McGeorge Bundy. *On Active Service in Peace and War* (1948).
15. Jennifer E. Sims and Burton Gerber. *Transforming U.S. Intelligence* (2005).
16. Michael Warner. "Wanted: A Definition of 'Intelligence'" (2007).
17. Professor Wilhelm Agrell, University of Lund. Keynote speech presented at the Kent Center Conference on "Understanding and Teaching Intelligence Analysis: A Discipline for the 21st Century" (2002).
18. Carl Von Clausewitz. *On War* (Trans. and ed. Michael Howard and Peter Paret, 1989).
19. Sun Tzu, translated by Ralph D. Sawyer. *The Art of War*.
20. Robert R. Leonhard. *The Principles of War for the Information Age* (1998).
21. Wayne Parsons. *Public Policy: An Introduction to the Theory and Practice of Policy Analysis* (1995).

TABLE 1. Primary Sources for Developing the Q-sample

Most of the intelligence definitions posited by the authors in Phase I presented either a knowledge-centered characterization espousing variations of Sherman Kent's knowledge-organization-activity definition or an IC-centered description distinguishing the IC from other knowledge-generating activities such as a weather bureau by its methods. Into this mix, the researcher introduced concepts proposed by military theorists – Clausewitz, Sun Tzu, and Leonhard – and a policy expert – Parsons – to represent the opinions of intelligence consumers.[6]

From the different approaches proposed for understanding intelligence, the author developed the Q-sample assertions regarding the necessity of a formal definition, the purpose of intelligence, debated elements of intelligence, and factors distinguishing intelligence as practiced by the IC from other knowledge-based activities. The Q-sample addressed topics such as covert actions and secrecy – elements of "intelligence" or products of the process, deception as an integral part of intelligence, and the relationship between the IC and its customers – decision-makers.

Three factors limit the completeness of the Q-sample: the completeness of references, the number of assertions in the sample (in other words, the ability of subjects to sort the list), and the preconceptions of the researchers that put the list together. In this study, the overabundance of posited definitions available far exceeded that which the author could consume in preparation of the Q-sample. Although a Q-sample may consist of hundreds of statements, the participants in the next phase can only effectively sort a limited set of statements. For this study, the volunteers that could not complete the Q-sort in less than 45 minutes did not complete it at all. While the participant-imposed size constraint may vary depending on external factors, such as top-down driven participation and personal interests, the researchers must consider this limitation when developing the Q-sample as it limits the range of opinions that can be presented. The pressure to maintain a manageable list also

works with the author's preconceived notions concerning the subject to constrain the Q-sample. In this case, the author refrains from presenting "obvious" or "trivial" assertions. Such trivial statements may, as this author discovered, provoke significant responses from the participants in the next two phases of the Q-methodology.

The two phases which followed Q-sample development explored the subjective opinions of intelligence officers and consumers regarding these topics. Their interpretation of each assertion added depth to the author's understanding of arguments put forth by theorists in the literature review.

PHASE II: THE Q-SORT AND ANALYSIS

The "Q-sort" process, as it is called, required the 66 participating intelligence professionals, military theorists, and academicians – ranging from recent hires to "gray-beards" – to rank the 62 Q-sample assertions into a bell-shaped matrix according to their level of agreement with each assertion relative to the rest of the declarations in the Q-sample, as shown in Table 2.[7] A context-based process, the Q-sort effectively filters out researcher biases inherent in creating the Q-sample.[8] The author then used *PQMethod*, a readily available and recommended freeware program, to perform the tedious Centroid calculations and graph-rotation mathematics necessary to group individuals by their preference or disdain for Q-sample assertions.[9] Using this software, the researcher identified five divisions of thought among the Q-sort participants as well as a set of common beliefs.[10]

Bin										
Agree	51									
4.5	26	8								
3.5	34	17	57	9						
2.5	27	52	11	49	6	30				
1.5	53	46	33	28	45	62	44	31		
0.5	2	1	50	10	43	61	35	36	47	48
-0.5	56	13	15	16	58	32	23	14	37	60
-1.5	40	25	5	4	41	21	24	12		
-2.5	18	22	59	54	3	29				
-3.5	7	19	20	38						
-4.5	39	55								
Disagree	42									

TABLE 2. In a typical Q-Sort, the participant lists the statement with which he/she most agrees at the top and least agrees at the bottom. Each assertion receives a point value (from +5.5 to -5.5) in the left-most column of its row in the analysis. Participants are grouped into divisions based on the pattern in which they distribute statements in the Q-sort.

Division 1. The distinguishing assertions in Division 1 paint intelligence as a fragile commodity—intellectually free, yet bounded by physical constraints and existing in a struggle with opposing agents for knowledge superiority. Subject to cultural, societal, organizational, political, and other forms of influence, intelligence is fragile. Thus, those who believe similarly to Division 1 regard the intellectual or physical separations between intelligence officers and their customers as essential to protecting the product. This division also prefers a knowledge-based definition that excludes missions such as undermining governments or facilitating assassinations. Work performed by intelligence officers contributes toward development of an intellectual product – knowledge, warning, forewarning, or some other intellectual commodity. Finally, Division 1 considers intelligence a resource-constrained competition – "The Great Game" – between intelligence organizations in which opponents strive to provide their customers a superior product – a "knowledge" advantage.

Division 2. Individuals in this group stress a necessarily strong partnership between intelligence professionals and decision-makers. Herein, the fear of irrelevance – of not comprehending their customer's dilemma – greatly outweighs the danger that outside forces might influence the IC's derived conclusions. Hence, Division 2 emphasizes the need to include the decision-maker – e.g., civilian leader, military commander, or operations officer – in the intelligence process and the intelligence officer in the decision process. Like Division 1, this group defines intelligence more by its products than the activities undertaken or the customers served. Unlike Division 1, however, Division 2 associates intelligence with the production of knowledge rather than how it is used. Thus, a covert mission undertaken by an intelligence agency qualifies as an intelligence mission *only if* it has a knowledge-generating objective. Lastly, despite the intertwined intelligence and decision processes, Division 2 believes intelligence professionals should control intelligence operations.

Division 3. A small group of participants confidently asserts that, with enough time, collection and analysis will successfully provide the most important knowledge necessary in the decision process. Likewise, Division 3 self-assuredly discounts the role an opponent's deceptions play in disrupting intelligence efforts, a logical conclusion given the beliefs in intelligence's ultimate success and in the supremacy of collection.[11] However, political influence and externally imposed controls constitute the greatest impediments to success; hence, Division 3 advocates for a stark separation between intelligence professionals and policy- makers.[12]

Division 4. The beliefs in this group hold strategic intelligence as distinct from tactical and operational intelligence because strategic intelligence requires collection methods and knowledge uniquely suited for

supporting national priorities. National decision-makers demand a focused collection of specific information conducted under a cloak of secrecy. To meet this demand and understand the context in which decisions take place, Division 4 – like Division 2 – advocates for a close working relationship between intelligence professionals and their customers. However, Division 4 also recognizes that, although essential, the veil of secrecy exists solely at the discretion of the national leadership – a product rather than an element of intelligence.

National decision-makers demand a focused collection of specific information conducted under a cloak of secrecy.

Division 5. While this category highlights beliefs put forth by the other divisions, the reasoning differs. For example, like Division 4, this classification believes that strategic intelligence differs from operational and tactical intelligence. However, Division 5 does not limit strategic intelligence's utility to strategic decisions; many users may benefit from one properly vetted, knowledge-based product regardless of their strategic, tactical, or operational mission. Accordingly, the intrinsic relationship between types of intelligence and various sets of customers requires that intelligence officers exert independent control of their resources, an operational reason for establishing a gulf between intelligence officers and decision-makers.

Consensus Statements. In addition to ascertaining the distinguishing statements for each division, *PQMethod* also identified five statements that scored consistently across the divisions. First, participants believe the definition of intelligence is independent of policies limiting intelligence activities. Secondly, deception attacks the decision-maker. Thirdly, security disrupts the competitor's collection efforts. Fourthly, collection assets require the bulk of intelligence resources. And finally, the "definition of intelligence" need not lead to a theory enabling resource management improvements. Interestingly, the second through fifth consensus statements directly and indirectly concern collection.

Summary. In Phase II, the Q-sort and analysis illuminated the disparity in the beliefs of a surveyed population consisting mostly of intelligence professionals. The five divisions developed from an analysis of the submitted arrays in Phase II often contradict each other. Furthermore, even when in agreement, the divisions differed in reasoning. Phase III examined the distinguishing concepts developed in Phase II.

PHASE III: THE POST-SURVEY INTERVIEWS

In Phase III, the researcher interviewed key participants (sometimes months after they submitted their survey) to clarify the reasoning they used during the Q-sort exercise.[13] The knowledge gained in Phase III also lessens the influence of the investigator's biases by providing alternative interpretations of the associations exposed by Phase II's graphical analysis. This final phase proved critical to understanding "intelligence" because it afforded the survey participants an opportunity to elaborate on their beliefs and, thereby, impart to the author nuances in their reasoning. Taken in total, the three-phased Q-methodology enabled the investigator to isolate, document, and analyze conflicting issues preventing development of a unifying definition for intelligence.

While the first two phases captured opinions delineating conflicting beliefs regarding the definition of intelligence, Phase III provided the key consensus and disagreements among participants that enabled the investigator to produce a theoretical framework for intelligence. In Phase III, the interviews revealed agreements regarding, first, a purpose for the definition and, second, the basic components of intelligence. Of these two areas, the former established the means to judge between conflicting opinions and led to "limiting factors" in a definition.[14] Described in the next section of this paper, difference of opinion regarding the boundaries of intelligence led to limiting factors that distinguish an intelligence theory for the IC from knowledge theories applicable to other forms of research. First, however, this study established a "lexical definition" developed from common principles of intelligence – process, knowledge, and decision.

The Purpose of an Intelligence Definition. Intelligence, as a tool of sovereigns, has existed without a formal definition for centuries. This historical fact again raises the question of why a definition is necessary – an issue broached through the Q-sample and elaborated upon during the interviews. However, in this study's sole area of unanimous concurrence, interviewees agreed that the IC needs a formal definition to efficiently manage intelligence resources. Participants lamented that, as it exists today, intelligence is informally defined more by the source of its funding or the missions it performs rather than through any formal document. Thus, any program or operation Congressionally-mandated to receive National Intelligence Program or Military Intelligence Program funds is "intelligence." By this definition, if an administration instructs the IC to collect and report on global warming or regional fresh water quality, these operations become intelligence.

The complexity of modern intelligence, its multi-billion dollar funding, and a complicated international political environment make the efficient application of the immense but limited resources imperative. Furthermore, without a definition, the "intelligence professional" is a baseless concept; a spy and a weatherman might both support national and strategic decisions, for instance. Should both be classified as intelligence officers? The answer, of course, depends on the definition of intelligence. Thus, regardless of how interviewees answered specific questions, they agreed that a definition of intelligence should differentiate that which is intelligence from that which is not and, furthermore, provide *measurable* components on which to anchor an intelligence theory.[15]

Intelligence, as a tool of sovereigns, has existed without a formal definition for centuries.

The Purpose of Intelligence – the Decision. Participants offered diverse opinions regarding intelligence's purpose, ranging from risk and resource management to producing knowledge. Although these perspectives appeared to offer no frame of reference by which to advance the debate, the interview process revealed that some participants believed intelligence served a consistent and understood purpose, i.e., risk or resource management, while others considered the ultimate objective of intelligence to be the prerogative of the decision-maker. These conflicting views, however, shared a common component – the decision.

Interviewees consistently described intelligence in context of the supported decision. Many asserted that, without a decision, the intelligence process produced purposeless knowledge; i.e., simple information. From the decision-maker's perspective, an interviewee posited, "The purpose of intelligence is to discern the proper response… to make the right decision." Another participant proposed that achieving a "decision advantage" is intelligence's primary purpose. A third interviewee translated this discussion into risk management terms. Intelligence, this person argued, gauges and mitigates risk and uncertainty by both understanding and influencing rivals. In this statement, the interviewee recognized that the decision advantage can also be achieved by attacking the opponent's decision-making – an insight placing disciplines such as deception, denial, security, and counterintelligence squarely within defined intelligence theory. Although interviewees advanced different opinions concerning the decision, in each discussion the "decision" clearly remained central to the definition of intelligence. Even interviewees who advocated for a stark separation between decision-maker and analyst acknowledged the need to understand the customer's ultimate decision to avoid becoming irrelevant.

The Central Role of Knowledge. Phase III confirmed knowledge and its production as fundamental within intelligence theory. Most participants affirmed knowledge's central role in intelligence.

Of particular interest, however, three interviewees explained why they rejected the premise that "At its most basic level, 'Knowledge' defines 'Intelligence.'"[16] Of these, two interviewees protested the inclusiveness of "knowledge" as a component of the definition. "Knowledge can be general," the first person stated. "There is no time quality to it. The word seems to assume it is always true." On the other hand, this interviewee continued, "Intelligence is knowledge about the enemy; it must be timely and it is usually limited by targeting." The second interviewee rejected the inclusiveness of knowledge preferring to focus on the IC's acquisition and processing of secret information as its primary "value-added" to the decision process. Both of these opinions, however, attempted to differentiate intelligence as practiced by the military and governments from other producers of knowledge such as weatherpersons. In both cases, knowledge remained a central tenet on which the two interviewees place limits. The third interviewee objected to defining intelligence by the "knowledge" produced rather than from the expertise intelligence officers needed to produce relevant knowledge. Anyone might produce a reasonably accurate first-order analysis of information, this participant argued. However, the layperson lacks the expertise needed to provide leadership with key relationships and to understand the context of information, recommendations, actions, reactions, and other intangibles that may reveal new perspectives on key decisions. Yet, this line of reasoning does not negate the importance of knowledge in the decision-making process. In fact, the expertise for which the third interviewee advocates simply affords consistently better knowledge than that created by untrained personnel. Thus, these three interviewees highlighted rather than diminished the importance of knowledge in a general definition of intelligence. Furthermore, knowledge presents a relevant and quantitative measure of intelligence as a product, e.g., reports produced and data collected, more than individual proficiencies.

A Process – Any Process. The Phase III discussions concerning process centered primarily on the assertion that "Information becomes intelligence when it has been processed – no matter how informally."[17] Although most participants accepted this supposition, the protests of four interviewees contributed important arguments needing resolution prior to accepting "process" in defining

intelligence. Two interviewees objected because the statement allows too much information to be classified as intelligence; the definition of the term becomes useless. However, this argument does not invalidate "process" as a component of a general, lexical definition; it simply accentuates that the IC needs a precise theoretical definition distinguishing its practices from others. Alternatively, the other two protesting participants considered "understanding" to be the primary product of intelligence; the "process" leads to understanding. Therefore, they posited, understanding and not process should be the defining component. The countering argument's reasoning resembles that regarding expertise vice knowledge. In this case, understanding is a function of process; in other words, the better the process, the greater the understanding. Additionally, defining intelligence with respect to a quantitative process instead of a subjective measure such as "understanding" yields a more practical theory by which the IC can manage its resources.

Rather than accepting *any* process, some interviewees posited the importance of learned skills such as a systematic approach to collecting and evaluating information as defining elements of intelligence. For instance, as intelligence officers accumulate experience and training, they gain the expertise and develop the discipline needed to rigorously and efficiently apply their organization's intelligence process. As one interviewee argued, the interaction with customers requires a disciplined approach acquired through training and experience by which intelligence officers can interface with policymakers and operations personnel while maintaining their objectivity. In other words, learned skills enable intelligence officers to produce superior products and provide insights where other disciplines might fail. Thus, like these interviewees, a casual observer might consider learned skills to be limiting factors that distinguish intelligence from common research.[18]

Yet, too many other professions conduct research using a similar formula for these traits to provide a useful means to differentiate intelligence. For example, the Office of Special Services' Research and Analysis Branch (R&A), credited with inventing the discipline of non-departmental strategic intelligence, was comprised of roughly 900 historians, economists, political scientists, geographers, psychologists, anthropologists, and diplomats under the leadership of Harvard historian William Langer.[19] Although areas of expertise developed over time, modern intelligence analysts require the same scholarly skills R&A recruited. Skills, therefore, do not appear to be a useful means by which to differentiate intelligence from other disciplines.

Additionally, learned skills vary in importance depending on the level of intelligence and the situation at hand. In tactical situations, as the element of time compresses, pressure drives analysts to make hurried assessments without the benefit of all the information they want or believe they need. Two interviewees suggested that some circumstances compress time to such an extent that one person – for example, the pilot or platoon leader engaged in tactical combat – assumes the functions of commander, operations officer, and intelligence officer. In such tactical situations, a minimalist approach to intelligence disciplines suffices to supplement combat training and experience and enables combatants to react to the fast-paced information assaulting their senses. The tactical case also illustrates why learned skills do not define intelligence. Because these skills vary from person to person, the subjective value of such skills might range from highly adept to amateurish. Yet, a minimal intelligence process still exists even if the practitioner executes it clumsily or chaotically. Thus, the general class of "intelligence" requires consideration of a process but not a learned skill.

The Lexical Definition of Intelligence. The Phase III interviews facilitated identifying general agreement on common components of intelligence; process, knowledge, and decision emerged as defining elements. These components characterized how surveyed participants use the term "intelligence." In its lexical form, *intelligence is any process producing knowledge for the purpose of making a decision.*

The common components of process, knowledge, and decision establish the areas in which the yet-to-be-developed intelligence theory provides quantitative insights enabling resource management.

This definition resembles one offered by Merriam-Webster's online dictionary – "the ability to apply knowledge to manipulate one's environment..."[20] The differences between this study's derived and the Merriam-Webster's proffered definitions stem from the purpose of the derived definition – to manage intelligence resources. To be a useful resource management tool, the theory requires intellectual access to the processes executed by the IC. Likewise, the theory must include the decision because, as many interviewees asserted, intelligence derives its value from the decision-making process rather than from manipulating the environment. The common components of process, knowledge, and decision establish the areas in which the yet-to-be-developed intelligence theory provides quantitative insights enabling resource management.

THE LIMITS OF "INTELLIGENCE" – THE FRAMEWORK FOR A THEORETICAL DEFINITION

Although an essential component, the lexical definition of intelligence encompasses too broad an idea on which to base a theory. As Wilhelm Agrell argues, "When everything is intelligence – nothing is intelligence."[21] Defining intelligence as practiced by the IC entails bounding what it is and clarifying what it is not – the "precising" step between a lexical and theoretical definition. Yet, intelligence professionals differ on what those boundaries include.[22]

Of the issues discussed during Phase III, three areas – secrecy, competition, and national policy – presented the most promising possible limiting factors. Once again, the interview process exposed countervailing arguments surrounding these issues. In the case of secrecy, some interviewees firmly asserted that the "value added" (e.g., that which differentiates intelligence from journalism) which intelligence provides to leadership rests in the secrets acquired and the shadows in which it operates. Nevertheless, others considered the IC's emphasis on secret information and covert actions as a reason for intelligence failures and loss of credibility.

In the second possibility, while most interviewees acknowledged that a competition between opposing intelligence organizations exists, many considered disciplines stemming from this competition – counterintelligence, denial and deception, security, and special operations (e.g., assignation, undermining foreign governments, etc.) – to exist outside the boundaries defining intelligence. Some participants viewed the current structure as sufficient justification for their beliefs. For example, responsibility for United States deception rests primarily with the Defense Department rather than with the IC. Others discounted such disciplines because their practitioners do not directly produce knowledge used in decision-making. Two interviewees, however, reasoned that activities diminishing or influencing an opponent's intelligence or decision process effectively improve one's own intelligence or decision advantage.

Finally, while most participants agreed the decision-maker defines intelligence's utility, only one posited on how this utility distinguishes intelligence from other activities. This interviewee suggested intelligence (as practiced by the IC) serves only the national leadership and national policy. Accordingly, this national service distinguishes collection activities performed by the CIA from missions performed by an Army reconnaissance platoon, a weatherman, or a reporter for *The New York Times*. Conversely, other interviewees rejected considering national service as a limiting factor because the IC serves decision-makers at all levels from tactical through strategic. Furthermore, they argued some knowledge applies to decisions at all levels while other pieces of information satisfy only the requirements of very specific consumers.

With the arguments for and against secrecy, competition, and national policy laid, the author required another means by which to select or reject the factors. Judging solely on the arguments presented simply places the study's conclusions on one side of a subjective debate and serves little purpose. Unlike the elements of the lexical definition, the researcher could not select or eliminate limiting factors based on the interviewees' reasoning alone because no common ground existed. To move beyond the former disagreements, the limiting factors must, in accordance with the purpose of the definition, differentiate intelligence activities from other forms of research. Fortunately, one interviewee arguing for a general definition and a second participant advocating a precise definition both challenged the author to consider specific scenario-based tests. Inspired by their suggestions, the author developed scenario-based tests upon which to judge the three limiting factor candidates.

The author sketched seven scenarios in which protagonists – with or without connection to the IC – conduct operations adhering to the lexical definition of intelligence. In brief, the scenarios depicted:

1. A boy asks friends to surreptitiously discover if a girl likes him.
2. A person deceives a new group of friends by concocting lies to hide a socially scarred past.
3. A corporation attempts to discover a competitor's secret formula.
4. A government sponsors environmental research regarding global warming.
5. An infantry reconnaissance platoon seeks to establish contact with the enemy.
6. A undercover law enforcement agent penetrates a foreign drug cartel outside U.S. borders.
7. An intelligence agency pierces a foreign state's leadership apparatus to discern that government's intended actions.

Using these scenarios, the author tested secrecy, competition, and national policy to determine which factors distinguished intelligence as practiced by the IC from the more general, lexical definition.[23] For example, a proposed factor that does not exist in the mundane (1-3) and government (4-6) scenarios, but is present in the IC scenario (7), gains credibility as a limiting factor. Conversely, a factor present in all the mundane and

government scenarios or that discounts the IC scenario loses standing.[24]

Secrecy. The author eliminated secrecy as a limiting factor because secrecy permeates the mundane boy-girl, hidden past, and corporate espionage scenarios. Individuals in mundane situations act to protect confidential facts or, in the corporate case, discover their competition's secrets. Of the government scenarios, secrecy only rejects the government-sponsored research scenario. Although one interviewee posited that reconnaissance platoons operate openly rather than secretly, secrecy failed to eliminate this scenario because the platoon acts in the larger context of its commander's secret plans. From the reconnaissance platoon's reporting and other sources of information concerning the enemy, the commander develops classified plans detailing why and where to attack, defend, surveil, reconnoiter, accept risks, and distribute limited resources.

Competition. As a limiting factor, competition fared better than secrecy for the mundane cases. Because the boy-girl and hidden past scenarios involve only one actor, competition successfully eliminates these two cases. Like secrecy, competition accepted the corporate espionage, reconnaissance, and law enforcement penetration scenarios while rejecting the government-sponsored research. Interestingly, except for correctly eliminating the first two mundane cases, "competition" performs identically to "secrecy." As a logical test, therefore, this result further eliminates "secrecy" as a possible limiting factor because secrecy's results are a subset of competition's results.

National Policy. The final factor, "national policy," eliminates cases not involving decisions of national consequence. Thus, this factor eliminates the boy-girl, hidden past, and corporate espionage scenarios. On the other hand, the national policy test accepts the government-sponsored research, reconnaissance, and law enforcement penetration cases.

Analysis Results.[25] The scenario-based testing resulted in the study's acceptance of "competition" and "national policy" and rejection of "secrecy" as limiting factors in a theoretical definition for intelligence. "Competition" and "national policy" provide complementary results that, together, eliminate the boy-girl, hidden past, corporate espionage, and government- sponsored scenarios. However, the Q-method did not generate another possible limiting factor to eliminate the reconnaissance and law enforcement penetration cases. To eliminate such cases, one interviewee suggested that Congressional budget lines carry more weight than operations when determining if a mission should adhere to intelligence or law enforcement policies. Alternatively, many interviewees distinguished intelligence from law enforcement operations because the IC protects its sources and knowledge while the Justice officials emphasize evidence – the witnesses and information used in courts. Likewise, the IC's concern regarding secrecy led some interviewees to differentiate "open" forms of collection, such as that which reconnaissance units produce or which comes from publicly available literature, from intelligence operations. However, this study refutes such distinctions as artificial, i.e., a matter of policy rather than practical experience and historical precedence.[26] Thus, extending the framework developed in this study to exclude law enforcement and openly executed operations reintroduces subjective arguments this study documented into the definition.

While not necessarily controlling law enforcement or military reconnaissance operations, the proposed intelligence definition leads one to conclude that elements of the IC should have cognizance of the data collected and information produced by government organizations outside their direct control. In other words, the IC should have awareness of law enforcement missions occurring in its areas of responsibility or producing information of national consequence. Furthermore, because these missions are logically comparable to IC operations, they should also adhere to the same legal restrictions imposed on IC assets when operating outside national borders.

PHASE III SUMMARY

The Phase III interviews delved into three fundamental concepts necessary for developing a working definition of intelligence, namely purpose, components, and limiting factors or constraints. At the most fundamental level, interviewees agreed the IC needed a definition and theory by which to better manage its resources. Consequently, the resulting definition should provide access to measurable components of intelligence – functions and areas through which managers adapt, correct, or improve the nation's intelligence apparatus. Regarding the purpose of "intelligence," however, subjects expressed a greater diversity of opinion. Many believed intelligence provides knowledge and considered its utility a matter for the end customer to determine. Others thought that intelligence's ultimate purpose lay in supporting leaders' resource allocation or risk mitigation decisions. These different opinions did not influence development of the theoretical definition because the two schools of thought lead to similar processes at the temporal point of decision-making and the two approaches exist within the "process" component of the definition – a detail of implementation rather than definitional element.

When constructing the definition, the purpose – in this case, enabling leadership to better manage intelligence resources – provided the primary catalyst behind its

development. The IC's resource management decisions entail differentiating, for example, what/who should receive funding versus what/who should not. While the lexical definition provides the theory's measurable components – the decision, process, and knowledge – this definition does not lead to a theory suitable for management decisions because, as one interviewee pointed out, the components of this intelligence definition do not solely exist within the context of the IC's activities. In other words, subjective determination of what is vice what is not intelligence remains the dominant factor in managing resources. Thus, we see the need for a precise definition in which limiting factors bound what lies within the IC's purview of intelligence and limits theory to the pertinent issues regarding intelligence. Interestingly, the limiting factors failed to exclude some operations not currently considered IC operations. These failures indicate areas in which the IC should have greater insight rather than a weakness in the derived definition.

CONCLUSION

This investigation yielded a framework for defining intelligence in terms of components – process, knowledge, and decision – and limiting factors – national policy and competition. Adding substance to the frame, this author proposes the following theoretical definition:

> *Intelligence is any process producing knowledge that might be used in making a decision OR influencing the processes, knowledge, or decisions of competitors AND in the face of competitors' efforts – real or imagined – to affect one's own processes, knowledge, or decisions in matters of national policy.*

Clearly, the proposed theoretical definition is weaker and more complicated than the derived lexical definition; i.e., *intelligence is any process producing knowledge for the purpose of making a decision*. Understandably, because the theoretical definition pertains to the realm of intelligence practiced by the IC, the relationship between the *process producing knowledge* and the *decision* must now recognize other knowledge-producing processes such as public polling, scientific findings, news reports, and personal experience. Hence, these "non-competitive" sources *might* equally dominate a leader's national decision-making process.[27] Likewise, inclusion of the competitive environment requires the theoretical definition to include attempts to achieve a competitive advantage either by upsetting a competitor's intelligence apparatus or protecting one's own intelligence operations from the machinations of a competitor. Naturally, this "game" constraint adds justifiable complexity to the lexical definition. Yet, conceptually, the theoretical definition remains a clean characterization of intelligence (as depicted in Figure 1).

Thus, this research led to a theoretical definition upon which to form intelligence theory – one which has, as intelligence expert Loch K. Johnson offers, "explanatory power, parsimony, and the attribute of falsifiability."[28] Using Q-methodology, the author distilled the subjective and sometimes emotionally charged opinions of intelligence professionals and theorists to logical arguments

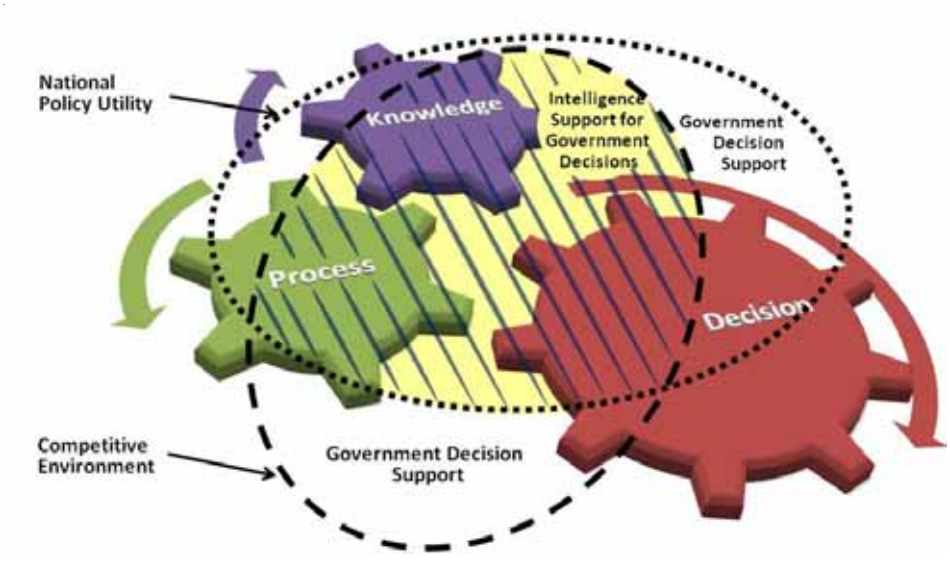


Figure 1. The Framework for a Theory of Intelligence. The three gears symbolize the lexical definition and the center, hashed region embodies the theoretical definition of intelligence.

that could be eliminated from a definition through analysis and scenario-based testing. The definition's components of decision, knowledge, and process provide the theory's measurable aspects. Concurrently, the limiting factors of competition and national policy focus the theory on the relevant issues, in this case, to the management of national intelligence.

Future research should proceed in three areas. First, following Q-methodology, researchers should execute a more robust investigation by developing assertions from a more complete set of opinion, then administering Q-sorts to and conducting interviews with a controlled set of U.S. and non-U.S. intelligence officers, military commanders, civilian decision-makers, and other intelligence consumers. Secondly, theorists should develop a quantifiable theory that "adheres" to definition in quantifiable terms. For example, Robert Leonhard, a military theorist, and Michael Warner independently proposed theories associating knowledge and risk. In Leonhard's treatise, a commander makes resource allocation decisions based on the information available.[29] The greater the accuracy of the commander's intelligence, the more precisely the commander distributes his or her forces. Conversely, a commander with poor or incomplete knowledge either over-compensates or accepts greater risks in his or her force deployments.

Decision and knowledge can be associated in measurable forms such as resources or risks.

On the other hand, Warner's proposal bypasses the resource discussion and correlates intelligence directly with risk management decisions.[30] Using Warner's construct, special missions, e.g., assassinations, undermining governments, deceptions, and denial activities (to include mundane security precautions), support the decision-maker by shifting risk onto an opponent. Although Leonhard's and Warner's ideas need not form the basis for an intelligence theory, their thoughts demonstrate that decision and knowledge can be associated in measurable forms such as resources or risks. Finally, analytical theorists should evaluate Q-mythology as a tool for addressing emotionally- and politically-charged debates within the IC. Used correctly, such a tool provides decision-quality understanding of controversial issues by parsing each emotion, belief, and fact into forms that enable comparative analysis.

Notes

[1] Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1949), xiii.

[2] Phillip J.H. Davies, "Theory and Intelligence Reconsidered," in *Intelligence Theory: Key Questions and Debates*, Studies in Intelligence series, ed. Peter Gill, Stephen Marrin, and Mark Phythian (London: Routledge, 2009), 201.

[3] Michael Warner, "Wanted: A Definition of 'Intelligence,'" *Studies in Intelligence* 46, no. 3, (2002), URL: <https://www.cia.gov/csi/studies/vol46no3/article02.html>, accessed 16 February 2007.

[4] Peter Gill, "Theories of Intelligence: Where are We, Where should We Go and How might We Proceed?" in *Intelligence Theory: Key Questions and Debates*, Studies in Intelligence series, Peter Gill, Stephen Marrin, and Mark Phythian, eds. (London: Routledge, 2009), 213.

[5] Garth Kemerling, "A Dictionary of Philosophical Terms and Names," *Philosophy Pages*, online only, URL: <http://www.philosophypages.com/dy/index.htm>; under the term "definition" then select "kinds of definition," accessed 16 December 2008. Kemerling describes three types of definitions pertinent to this research, namely lexical, precising, and theoretical. The first of these, the lexical definition, reports how a term is used. The second, the precising definition, attempts to reduce vagueness by stipulating limiting factors onto a lexical definition. Finally, the theoretical definition places a precising definition into the context of a theory.

[6] These two groups inspired 85% of the Q-sample. The inspiration for the remaining 15% came from discussions with instructors and students at the National Defense Intelligence College.

[7] Maarten Warnaars and Willy Pradel, "A Comparative Study of the Perceptions of Urban and Rural Farmer Field School Participants in Peru," *Urban Harvest Working Papers Series, Paper 4* (Lima: International Potato Center, May 2007), URL: <http://www.cipotato.org/publications/pdf/003796.pdf>, 8-9, accessed 25 July 2008. Q-methodology proponents assert that the views of a small group encompass those of an entire community. Consequently, as few as forty participants can provide a sufficient group from which to draw conclusions.

[8] Steven R. Brown, *Political Subjectivity: Applications of Q-methodology in Political Science* (New Haven, CT: Yale University Press, 1980), 19 and 46-47.

[9] Dr. Steven Brown, Professor, Department of Political Science, Kent State University, e-mail to author, subject: "Q-sort," 27 August 2008.

[10] According to Dr. Brown, the process of distinguishing between groups of thought can be somewhat arbitrary. The technique described in *Political Subjectivity* and emulated by *PQMethod* leaves the determination of how many divisions to generate from a set of data to the subjective discretion of the researchers (Brown refers to the divisions as "factors"). This subjectivity, however, occurs outside the topic area being researched. In this study, for example, the author determined that limiting the analysis to fewer than five divisions placed too many distinguishing assertions into a group. On the other hand, isolating more than five divisions placed too few statements in each. In both cases, the author could not draw reasonable conclusions from the resulting data. Only in the data generated through the five divisions did the author find the relationships discussed. In principle, the same data might yield different results if examined by a different researcher or if the author continued the Centroid calculations and graph-rotations to isolate different relationships. Equally as likely, the same data may

reveal information regarding additional issues in the topic area. This data-mining attribute of Q-methodology does not nullify the conclusions derived in research.

[11] An observer may view the terms "confidently" and "self-assuredly" employed in this analysis as an overstatement of the data. A more accurate portrayal of Division 3 could arguably restate this confidence as "an understanding of intelligence biased in its potential contribution to the decision process." However, such a wordy description obfuscates the relationships derived when using "confidently" and "self-assuredly."

[12] Opinions put forth by the four individuals making up Division 3 stand in stark contrast to those expressed in the other four Divisions. Five of the top seven statements with which Division 3 most agreed directly conflicted with the sentiments expressed by most participants. 40% of survey respondents least correlated – most disagreed – with the opinions listed in Division 3. Yet, this contradiction reveals a unique perspective on intelligence.

[13] Ideally, the interview process should occur immediately upon completion of the survey. Nonetheless, during direct questioning, survey participants usually recalled why one statement scored better or worse than others. That the ability to reconstruct reasoning occurred uniformly among participants aligns well with the claims of Q-methodology proponents who argue the process is repeatable – with respect to each participating individual – and is, therefore, a quantifiable measure of each participant's subjectivity.

[14] A "precising" definition narrows or limits the more general lexical definition. A "theoretical" definition performs the same function as a "precising" definition; but, it does so in the context of a theory. In this case, the investigator has proposed a precising definition as a starting point from which to develop intelligence theory.

[15] The goal of producing a theoretical definition for intelligence dictates the need for measurable components. Otherwise, the theory produced would not be testable – i.e., another opinion.

[16] Lieutenant Colonel Milton E. Diaz, USAF, "A Framework for Defining Intelligence in Support of National Security" (MSSI thesis chaired by Mr. Jon A. Wiant, Washington, DC: National Defense Intelligence College, February 2009), 142. Statement #4 of the Q-sample.

[17] Diaz, 149-150. Statement #31 of the Q-sample.

[18] Many of the authors examined in Phase I discussed specific skills as opposed to the generalized terms such as "discipline" and "expertise." In Phase III, the interviewees revealed a need to consider learned abilities such as "discipline" and "expertise."

[19] Michael Warner, "Research & Analysis," *The Office of Strategic Services: America's First Intelligence Agency* (Public Affairs, Central Intelligence Agency: Washington, DC, 2000), URL: < https://www.cia.gov/ library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/oss/art04.htm, accessed 22 February 2010.

[20] *Merriam-Webster's Online Dictionary,* s.v. "Intelligence," URL: < http://www.merriam-webster.com/dictionary/intelligence >, accessed 6 January 2009. The online dictionary offers more definitions.

[21] Wilhelm Agrell, Professor, University of Lund, keynote speech presented at the Kent Center Conference on "Understanding and Teaching Intelligence Analysis: A Discipline for the 21st Century" (Washington, DC, 23 May 2002). Edited version available online: "When Everything is Intelligence – Nothing is Intelligence." *Occasional Papers* 1, no. 4, October 2002. URL: < https://www.cia.gov/library/kent-center-occasional-papers/pdf/OPNo4.pdf>. Accessed 24 November 2008.

[22] Interestingly, in Phase II, participants reacted positively to 62% of statements defining components – the pieces of intelligence – as compared to 18% of assertions limiting intelligence.

[23] The author conducted the scenario-based assessment after completing field research. The participants did not take part in this analysis except by forming the basis – through the Q-methodology – for establishing the criteria used and obtaining the factors examined.

[24] None of the factors examined incorrectly rejected the IC scenario (#7).

[25] At this point, the author could develop either of two conclusions, namely, that the model is wrong or incomplete, or that the commonly accepted reasoning for what constitutes intelligence in the United States, regarding, for example, the reconnaissance and law enforcement penetration cases, results from artificial distinctions.

[26] For example, although the methods employed differ, secret police forces, reconnaissance units, and spies may be used to accomplish a similar objective such as obtaining knowledge of an enemy's disposition. Historical examples of secret police forces such as ancient Sparta's *Krypteia*, medieval Germany's *Vehmgericht*, the Russian Tsar's *Okhran*a, and Heinrich Himmler's *Schutzstaffel* (SS) abound in general reference books.

[27] The sources are non-competitive because there does not exist an outside agency bent on corrupting or preventing the collection of data.

[28] Loch K. Johnson, "Sketches for a Theory of Strategic Intelligence," *Intelligence Theory: Key Questions and Debates*, Studies in Intelligence series, Peter Gill, Stephen Marrin, and Mark Phythian, eds. (London: Routledge, 2009), 33.

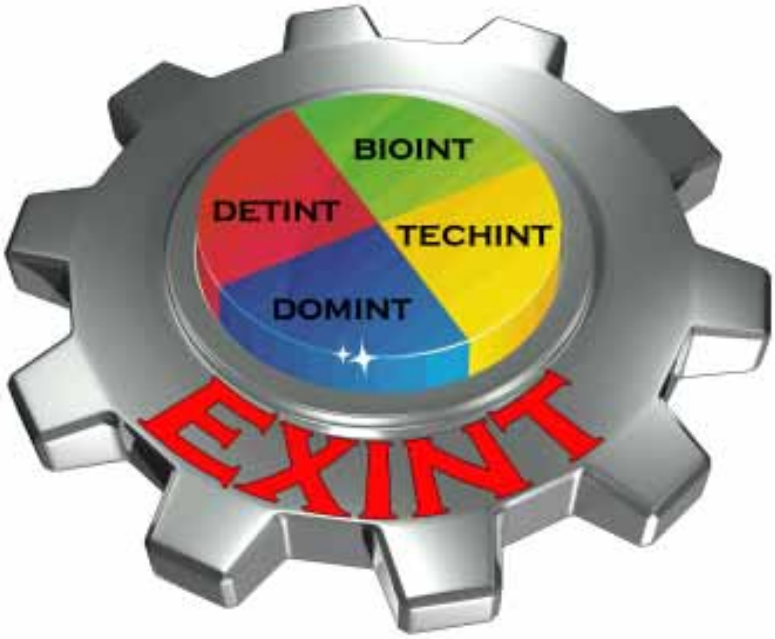
[29] Robert R. Leonhard, *The Principles of War for the Information Age* (Novato, CA: Presidio Press, 1998), 251-255.

[30] Michael Warner, "Intelligence as Risk Shifting," in *Intelligence Theory: Key Questions and Debates*, Studies in Intelligence series, Peter Gill, Stephen Marrin, and Mark Phythian, eds. (London: Routledge, 2009), 19-24.

Milton E. Diaz is an intelligence officer at the Defense Intelligence Agency. A retired Lt Col in the U.S. Air Force, he served as a strategic missile launch officer, acquisition officer, and modeling and simulation specialist. He was awarded a BS in Computer Engineering by the University of California; an MS in Computer Science (Artificial Intelligence) by the Air Force Institute of Technology; and a Master of Science of Strategic Intelligence (MSSI) by the National Defense Intelligence College. The views expressed in this paper are the personal ones of the author and do not reflect the official policy or position of the Defense Intelligence Agency, the Department of Defense, or the U.S. Government.

Exploitation Intelligence (EXINT):
A New Intelligence Discipline?

by MAJ (USA) Charles D. Faint



DISCLAIMER

This article is an outgrowth of research done in support of degree requirements for the National Defense Intelligence College and is intended to provide a starting point for discussion, not to draw definitive conclusions or to aggressively advance a specific position on the subject. Unless otherwise specified, the information and views expressed in this article are those of the author and do not reflect the official policy or position of the U.S. Intelligence Community, the National Defense Intelligence College, the Department of Defense, or the U.S. government.

FRAMING THE PROBLEM

At the 2009 Document and Media Exploitation (DOMEX) Conference, hosted by the National Ground Intelligence Center, Colonel Joseph Cox argued for the establishment of DOMEX as a separate intelligence discipline, which he termed "Document and Media Intelligence" (DOMINT). At that conference and in a subsequent article published in the *Military Intelligence Professional Bulletin*,[1] COL Cox laid out his reasoning for placing DOMEX on par with the seven existing intelligence disciplines.[2] As I considered COL Cox's ideas and related them to my own observations in Iraq and Afghanistan, and to my experiences as a career Army intelligence officer, I was convinced of the utility of DOMINT. As I thought more about it, however, I began to wonder if DOMINT could in fact stand alone as an intelligence discipline, or if DOMINT would better serve the Intelligence Community (IC) as a component or sub-discipline of an entirely separate intelligence discipline, one centered on the exploitation of captured enemy personnel and materiel. I called this potential new discipline "Exploitation Intelligence," or EXINT.

The process of exploiting captured enemy personnel and materiel for intelligence purposes dates back thousands of years. Perhaps the first example comes from the Egyptians,

who exploited the captured iron weapons of their Hittite opponents in order to improve their own weapons made of inferior bronze.[3] The fledgling U.S. Army made use of captured enemy personnel, equipment, and documents during the American Revolution, a practice continuously expanded upon and continued to the present day. Information derived from the interrogation of captured enemy personnel contributed to the capture of Saddam Hussein,[4] the death of Abu Musab al Zarqawi,[5] and the killing of Osama bin Laden.[6] These examples underscore the utility and value of the exploitation process and intelligence derived from exploitation methods.

FINDING COMMON GROUND

In researching this subject it became apparent that the IC is not always in agreement on descriptions, doctrine, or definitions related to intelligence. For example, the Army states there are nine intelligence disciplines, while the joint military publication on intelligence states there are seven[7] and the FBI promulgates five "intelligence collection disciplines."[8] Furthermore, the Department of Homeland Security advocates for the creation of "Homeland Security Intelligence" (HSINT) and also makes mention of "security intelligence," "domestic intelligence," and "domestic national security intelligence."[9]

Given the inconsistency of common terms within the IC, I had to decide on a common reference in order to deconflict terms for this article. Because elements of the Department of Defense (DoD) comprise more than half of the 17 organizations of the IC (16 members plus the Office of the Director of National Intelligence),[10] I felt it was logical to use DoD references in situations where I encountered conflicting information. As a result, this article relies on joint military publications, specifically Joint Publication (JP) 2-0, "Joint Intelligence," published in June 2007, as the most authoritative source of doctrinal intelligence-related information. In cases where a useful contrast to JP 2-0 is provided by other sources, or where existing doctrine falls short, this article provides those sources as well as alternative definitions and descriptions based on compilations of sources.

THE PURPOSE OF INTELLIGENCE

To adequately assess the potential value of EXINT as a separate intelligence discipline, an important starting point involves an understanding of the purpose of intelligence. Unfortunately, there does not appear to be a consistent description of this purpose across the IC. Some definitions of the purpose of intelligence are very detailed and complex, while some can explain it in a handful of words. Most military definitions revolve around some version of the phrases "inform the commander" or "drive operations." This line of thinking is typified by the Army's description of the purpose of intelligence:

> *The purpose of intelligence is to provide commanders and staffs with timely, relevant, accurate, predictive, and tailored intelligence about the enemy and other aspects of the AO. Intelligence supports the planning, preparing, execution, and assessment of operations. The most important role of intelligence is to drive operations by supporting the commander's decision-making.*

Additionally, the purpose of intelligence as specified by JP 2-0 is to:

> *…inform the commander; identify, define, and nominate objectives; support the planning and execution of operations; counter adversary deception and surprise; support friendly deception efforts; and assess the effects of operations on the adversary.*[11]

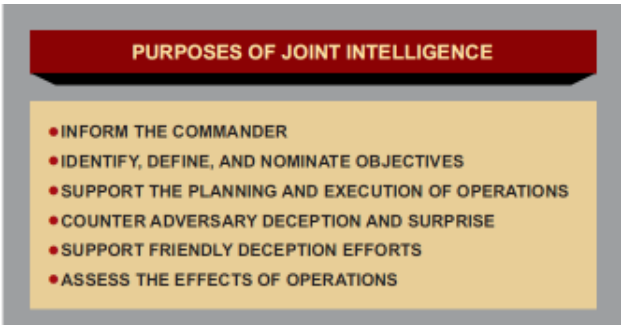


Figure 1: Purposes of Joint Intelligence. Source: JP 2-0.

This definition was one area in which I felt JP 2-0 was lacking because it is military-centric and cannot be easily applied across the civilian components of the IC. The JP 2-0 definition also rather conspicuously omits the mission of counterintelligence. Moreover, while the above definitions are sufficient in military applications, they do not accurately represent the expectation most U.S. citizens have of the intelligence enterprise, which in most cases might simply be to prevent surprise. A concept of intelligence that is better suited for the entire IC can be found in Mark Lowenthal's oft-cited textbook, *Intelligence: From Secrets to Policy*:

> *Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policy makers; the products of that process; the safeguarding of these processes and this information*

by counterintelligence activities; and the carrying out of operations as requested by lawful authorities.[12]

I felt Lowenthal's definition was much better than that in JP 2-0, but I felt it was still somewhat lacking. Combining all of the available definitions of the purpose of intelligence, I compiled the following:

The purpose of intelligence is to enable "decision advantage"[13] by disseminating timely, accurate, predictive and contextualized assessments of the operational environment in order to provide early warning and prevent surprise, and to prevent the compromise of intelligence products and the sources and methods of collection.[14]

The above definition encompasses all of the existing intelligence disciplines, including CI, which as previously noted seems to have been omitted in the military definitions of the purpose of intelligence. It also makes the definition more all-encompassing by removing the stipulation that intelligence is for "commanders" or "policy makers," thereby recognizing the fact that anyone can be a legitimate consumer of intelligence, including other intelligence professionals.

Some terms in the above definition of the purpose of intelligence warrant further explanation. The best definition I found for "decision advantage" is the "*…ability of the United States to bring instruments of national power to bear in ways that resolve challenges, defuse crises, or deflect emerging threats.*"[15] This is significant because intelligence exists not for its own sake, but in order to provide decision-makers with the best information possible, so that they may make the best decision possible. Additionally, in the definition above, "early warning" provides intelligence related to specific anticipated events, such as fixing the enemy in time and space in order to make him targetable, while "preventing surprise" refers to the efforts to determine and mitigate enemy plans and intentions. In short, "early warning" is focused on the enemy, while "preventing surprise" is friendly forces-centric.

THE INTELLIGENCE DISCIPLINES

With the purpose of intelligence established, we can move on to a description of what makes an intelligence discipline, and explore the seven joint intelligence disciplines currently in existence. An intelligence discipline is "*…A well defined area of intelligence planning, collection, processing, exploitation, analysis, and reporting using a specific category of technical or human resources.*"[16] According to JP 2-0, the extant joint intelligence disciplines are counterintelligence (CI), human intelligence (HUMINT), geospatial intelligence (GEOINT), open-source intelligence (OSINT), signals intelligence (SIGINT), measurement and signature intelligence (MASINT), and technical intelligence (TECHINT).[17] Within these disciplines are several sub-disciplines, as shown in the following chart:

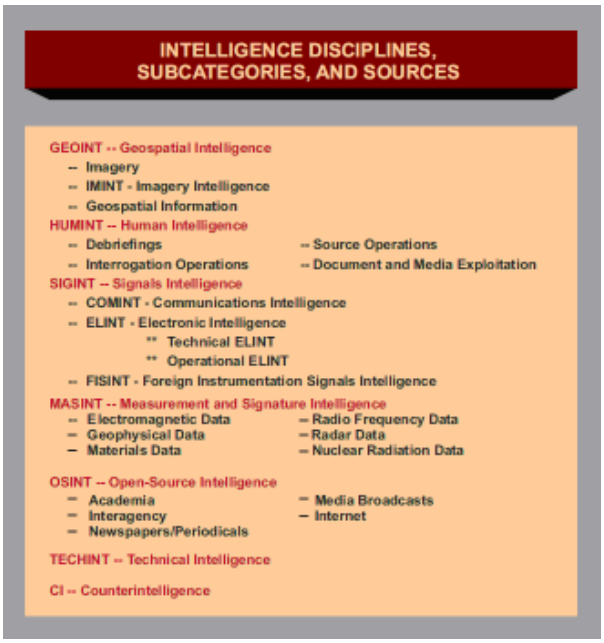


Figure 2: Intelligence Disciplines and Sub-Disciplines. Source: JP 2-0, page I-6.

The way the IC distinguishes intelligence disciplines from one another is based on "how" the information is collected, instead of "what" is collected. In so doing, it is easy to see how strong cases can be made that the same collection effort might fall into different intelligence disciplines, or "-INTs." A useful example may be to consider a telephone conversation between two people. If one of those individuals uses the phone to pass along information to a witting recipient on the other end of the line, we would recognize that as HUMINT. However, if that same conversation were intercepted by a third party, the information garnered would be SIGINT. Utilizing a similar example, if a photograph of a military installation is taken by a classified overhead collection platform, it would be IMINT. But if a photo of the exact same installation were downloaded from the Internet, it would be considered OSINT; if it was delivered by a paid source, it would be HUMINT. A radar return showing an enemy armored convoy is considered IMINT, but a case can be made that, since radar measures the return of radio waves, the information is collected as a result of MASINT.

The above examples are far from semantic arguments; accurate descriptions of intelligence disciplines are tied to

proper collection and classification of information, as well as training, equipping, and fielding the right kinds of intelligence platforms and personnel. It is important to accurately categorize intelligence information in order to apply the correct resources against it and to utilize it to its fullest extent. It is with that in mind that I will now turn my attention toward explaining EXINT.

DESCRIPTION OF EXINT

Joint Publication 1-02 explains "exploitation" in part as "*taking full advantage of success in military operations, following up initial gains, and making permanent the temporary effects already achieved*," and "*taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes*."[18] This is a very useful definition to use when exploring the potential utility of EXINT. By exploiting captured enemy personnel and materiel, EXINT would make permanent the temporary gains achieved in the seizure of those personnel and equipment by extracting the maximum value from those items. This in turn would allow U.S. forces to take "full advantage" of what has "come to hand" by providing more thorough intelligence information to support decision-makers at all levels. Combining the definition of exploitation with the definition of the purpose of intelligence provided earlier in this article and putting it into the context of "exploitation intelligence," the definition of EXINT is as follows:

> *The process by which captured enemy personnel and materiel are exploited for intelligence purposes as part of the all-source effort to provide "decision advantage" to decision-makers at all levels. EXINT consists of four parts: biometrics (BIOINT), detainee interrogations (DETINT), document and media exploitation (DOMINT), and technical intelligence (TECHINT).*

If EXINT were to become a separate -INT, what would comprise the new discipline? To begin with, TECHINT, already established as a separate intelligence discipline, would become a sub-discipline and be subsumed under EXINT. EXINT would also encompass interrogations, which would become a separate sub-discipline: detainee exploitation, or "DETINT." Document and media exploitation intelligence, or "DOMINT," would move from HUMINT, as would biometrics intelligence or "BIOINT." TECHINT, DETINT, DOMINT, and BIOINT would comprise the four elements of EXINT.

EXINT is differentiated from other -INTs by the way in which it is gained from personnel or enemy equipment that is in friendly hands; information collected "in the wild" belongs to another discipline. For example, when the exploitation of a captured enemy communication device yields a specific contact number, then that is EXINT. When collection is applied against that number, the resulting information is SIGINT. Information from an enemy detainee is EXINT, while information elicited from an enemy politician or soldier by a collector is still HUMINT. Intelligence information gained from the technical evaluation of a missile fired by the enemy would be MASINT, whereas the technical information derived from that same missile would be EXINT if it were to occur while the missile was in friendly hands.

If EXINT were to become its own discipline, little in doctrine would have to change. CI, GEOINT, OSINT, and MASINT would likely be completely unaffected by EXINT. HUMINT would lose three components: biometrics, interrogations, and DOMEX. Doctrine would need to further change to reflect the establishment of BIOINT, DOMINT, and DETINT as official sub-disciplines of EXINT. The -INT most affected by EXINT would be TECHINT, because it would lose its status as an independent discipline and would fall under EXINT. HUMINT would also be affected because interrogations are currently a HUMINT function. Change would be required in order to implement EXINT, but most if not all of these changes should be transparent to the majority of the IC and the intelligence consumers that the IC supports. If JP 2-0 were revised to take the above changes into account, it might look something like this:

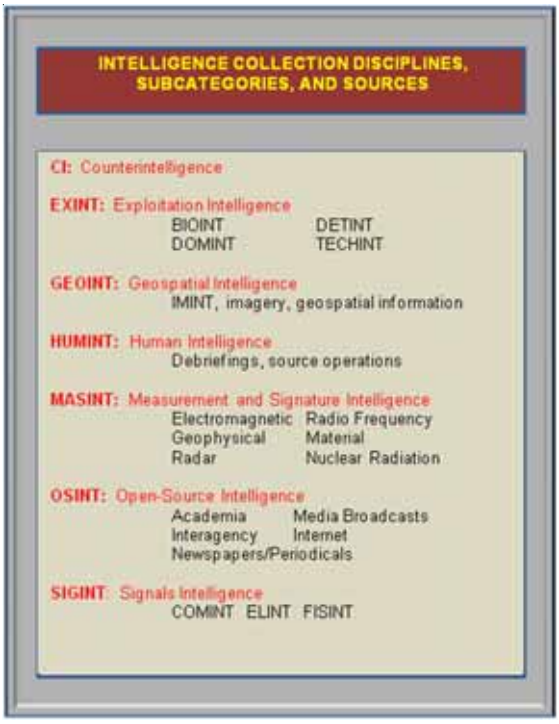


Figure 3: Revised JP 2-0 Intelligence Disciplines. Source: Author.

CONCLUSION

If the purpose of intelligence is to enable "decision advantage" at all levels, and if an intelligence discipline is defined as collection in a "*specific category of technical or human resources*," then EXINT (comprised of BIOINT, DETINT, DOMINT, and TECHINT) would appear to be able to stand on its own as a new intelligence discipline.

Although the potential value of EXINT is clear through myriad historical examples, more research is required in order to determine if the cost/benefit analysis of establishing a new intelligence discipline weighs in favor of EXINT, or whether the tasks that this article ascribes to EXINT are better accomplished by the intelligence disciplines already in existence. At this point however, when considered against the doctrinal definition of what comprises an intelligence discipline, the validated contribution of intelligence gained from exploitation methods, and the intuitive utility of grouping "like functions" together, it appears likely that EXINT is warranted.

Notes

[1] Cox, Joseph, "DOMEX: The Birth of a New Intelligence Discipline," *Military Intelligence Professional Bulletin*, April-June 2010, p. 22.
[2] Joint Publication 2-0, "Joint Intelligence," June 2007, http://edocs.nps.edu/dodpubs/topic/jointpubs/JP2/JP2-0_950505.pdf *(accessed 4 October 2010).*
[3] Clark, Robert, *The Technical Collection of Intelligence*, CQ Press, Washington, DC, 2011, p. 247.
[4] BBC news, "How Saddam Hussein Was Captured," 15 December 2003, http://news.bbc.co.uk/2/hi/3317881.stm (accessed 20 April 2011).
[5] Bowden, Mark, "The Ploy," *The Atlantic*, May 2007, http://www.theatlantic.com/magazine/archive/2007/05/the-ploy/5773/ (accessed 20 April 2011).
[6] Goldman, Adam, and Apuzzo, Matt, "How Was Osama bin Laden Caught? One Small Mistake," The Associated Press, 2 May 2011, http://www.uticaod.com/news/x449043929/How-was-Osama-bin-Laden-caught-One-small-mistake (accessed 4 May 2011).
[7] Joint Publication 2-0, "Joint Intelligence," Department of Defense, June 2007, p. I-5.
[8] FBI, Director of Intelligence, "Intelligence Collection Disciplines (INTs)," http://www.fbi.gov/about-us/intelligence/disciplines (accessed 20 April 2011).
[9] Randol, Mark A., "Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches," Congressional Research Service, 14 January 2009, p. 6.
[10] Intelligence.gov, "About the Intelligence Community," http://www.intelligence.gov/about-the-intelligence-community/ (accessed 28 April 2011).
[11] JP 2-0, p. I-3.
[12] Lowenthal, Mark, *Intelligence: From Secrets to Policy*, 4th ed., CQ Press, Washington, DC, 2009, p. 8.
[13] J.M. McConnell, "Vision 2015," (undated) http://www.dni.gov/Vision_2015.pdf (accessed 13 April 2011).
[14] Refined definition of the purpose of intelligence, compiled by the author from a variety of sources.
[15] "Vision 2015," p. 8.
[16] Joint Publication 1-02, "Department of Defense Dictionary of Military and Related Terms," Department of Defense, 17 October 2008, p. 181.
[17] Joint Publication 2-0, "Joint Intelligence," June 2007, http://edocs.nps.edu/dodpubs/topic/jointpubs/JP2/JP2-0_950505.pdf *(accessed 4 October 2010).*
[18] JP 1-02, p. 132.

[Author's Note: "EXINT Cog" on title page courtesy of Lisa Antram.]

MAJ Charles D. Faint is a career Army intelligence officer with extensive experience in special operations and over 16 years of service. His most recent operational assignment was with the Joint Special Operations Command at Fort Bragg, NC, where he served as a troop commander and executive officer. He also held various command and staff positions within the 5th Special Forces Group and the 160th Special Operations Aviation Regiment. He has deployed a total of seven times to Iraq and Afghanistan and also served peacekeeping tours in Egypt and the Republic of Korea. In addition to his undergraduate degrees in engineering and technical communication from Mercer University, MAJ Faint holds a Master of Arts in Management and Leadership from Webster University and a Master of Science of Strategic Intelligence from the National Defense Intelligence College. His next assignment is advanced civil schooling at Yale University, where he will study International Relations en route to a teaching assignment in the Department of Social Sciences at West Point. MAJ Faint welcomes feedback on his article and can be reached via e-mail at charles.faint@us.army.mil.

Latte Intelligence:
The Divorce of Shock Creativity and Special Information Operations

by R.J. Godlewski

Shock warfare, perhaps more appropriately termed "action propaganda,"[1] remains the most dynamic employment of a creative device for combat operations. Though admittedly of little lasting strategic value,[2] such implementations of surprise are designed primarily to instill an immediate sense of uncertainty within an adversary through forcing either a "fight or flight" posture.[3] These are the tactics often utilized by "barbarians" – in other words, the allegedly less civilized people "who will do anything, absolutely anything to gain victory."[4] Given this reality, the most effective application of counter-shock to such an enemy's organization rests in the silencing of its innovators and herein lays the intrinsic value of special information operations (SIO).

Practitioners of military intelligence, surveillance, and reconnaissance (ISR) operations, for their part, aim squarely for that ability to "strike where we want when we want – and nobody can stop us."[5] The obvious value of this capability rises significantly in such arenas as modern urban operations where "the one commodity a close-combat soldier or Marine demands most is knowledge of the enemy waiting around the street corner in ambush."[6] Such an intimate courtship between absolute aggressiveness and infinite knowledge existed since at least the time of Chinggis (Genghis) Khan.[7] Today, unfortunately, this long-lived marriage rests within a bitter six-decade divorce battle pitting those who believe – as General Douglas MacArthur once lamented – that it is "unconscionable to wage war without the will to win" against those who believe that the existence of an enemy who will torture and rape as a sport, slaughter children along with the elderly, and break treaties with no more care than taking a breath remains a subject much debated.[8]

As with any comparable marital breakup, the primary victims are the union's offspring – in this particular case, the American fighting men and women – who are left feeling disjointed and confused over their future, i.e., soldiers who are struggling to come to terms with the elusiveness of killing bona fide enemies as an official doctrine.[9] To ease such filial disenchantment, senior military and political leaders often sought ways in which to pacify their concerns through the near exclusive use of technological and informational advancements as a means of waging war.[10] Unfortunately, technology only becomes more impotent the closer it progresses toward the actual firing line.[11]

THE LIFEBLOOD OF WAR

For brevity, a simple supposition regarding the need to engage in combat operations exists – they are fought: (1) to destroy an enemy's ability to wage war; (2) to destroy an enemy's will to wage war; and (3) to convert former adversaries into allies.[12] Without success in achieving all three of these objectives, conflicts remain simmering and can flash anew with the slightest agitation. It is for this very reason that North Korea, China, and Russia remain irritants today while Japan and Germany have learned to become allies of the United States. If accepted that the foregoing conditions reflect an honest assessment for the involvement of the United States in regional or international combat operations, then that acknowledgement also accepts that America's track record since the conclusion of the Second World War represents one of rather disastrous results:

- America's mounting reliance upon precision weaponry has distanced indigenous peoples from accepting responsibility for wars waged on their behalf;[13]
- America's culture is largely ignorant of the historical basis for "barbarism" in certain enemies' will to fight. Rarely is mention made of such atrocities as soldiers being buried alive or having their heads nailed to trees (Germans against Romans); young women and religious nuns being raped in front of hostages (Mongols against Russians); or captives simply being disemboweled (Zulus against British);[14]
- America's devotion toward the prospect of earning the respect of its past enemies occasionally gets its troops killed during the present.[15] Many of these past adversaries remarked on just how naïve American soldiers new to close quarters combat were, and both German and Japanese veterans marveled at how quickly U.S. soldiers sought to mend relations with their captives and bond with them once the battle was over.[16]

American national will thus remains predicated upon the concept of convenience; civilians remain motivated to fight only when lives are inconvenienced by an enemy. Otherwise, they prefer to engage solely within economic or leisure pursuits. Even American fighting forces, those on the frontlines of combat, often find it difficult to believe that someone "unknown" really wants to kill them.[17] Fortunately, however, American soldiers and Marines often possess an innate creativity, innovativeness, and initiative that compensate for society's lack of formally preparing them for just such encounters.[18]

CREATIVE FORCE-MULTIPLICATION

In the context of war and combat, there are eight basic elements of creative device that serve as force-multipliers in situations where both human and material assets are limited (**See Table 1, Figure 1**). The military leader who does not exploit these traits will severely handicap commanded forces at the mercy of those enemies that more fully utilize these resources. Inasmuch as the Army Chief of Staff, General George Decker, erroneously believed in 1962 that "Any good soldier can handle a guerrilla," just any "good soldier" or even experienced general officer cannot handle a more innovative adversary.

Like guerrillas, creative personalities live, breathe, and die within a "unique terrain" – artistic talent being much more than just a job or career; it is a virtual lifeblood or "mother's milk" that cannot be squashed by artificial means. When serving the opposing cause, such personalities can remain a formidable enemy for the duration of their lives. Therefore, counter-creative effort must take into consideration that no amount of training or education will enable the uninitiated to corral the behavior of those born and bred to adapt.

THE FAILURE OF "HEARTS AND MINDS"

All humans seek Messianic salvation of some form, for they seek purpose in life and will readily adhere to whichever system of beliefs or proponent best matches their expectations of a purposeful future. Whether an individual will follow an Osama bin Laden or a President Barack Hussein Obama depends primarily upon which choice provides the most inspirational – read that, *creative* – message. In its own deliverance, the West fails

Type of Exploitation	Characteristics	Historical Samples
Necessitated Creativity	Innovation caused by need.	Carl Gustav von Rosen's use of "Minicoin" aircraft against Nigerian Army targets in 1969.[19]
"Drive By" Creativity	Innovation intended to silence adversaries through decisiveness and brutality.	Modern suicide bombers.[20]
Offensive Creativity	Innovative practice designed to maintain pressure upon an enemy.	"Shock and Awe" prior to the 2003 invasion of Iraq.[21]
Defensive Creativity	Innovative practice intended to alleviate pressure.	U.S. landings at Inchon during the Korean War.[22]
Psychological Creativity	Innovation intended to confuse and disorient.	The British use of a helium-filled, luminescent soccer ball dropped on a Nazi airfield in WWII.[23]
Technological Creativity	Innovation which permits adaptation through artificial means, particularly that which creates systems and events where none truly exists.	Orson Welles' 1938 *War of the Worlds* broadcast; Iran's 2008 "Composite Image" missile launches.[24]
Instructional Creativity	Innovative practice in human adaptation and training.	"Word Puzzles" used to train household goods truck drivers; role-playing exercises.
Directorial Creativity	Innovation in leadership, which can galvanize a nation or a unit to achieve the unthinkable.	President Kennedy's pronouncement to land men on the moon by the end of the decade.[25]

Table 1. Eight Methods of Creative Exploitation.

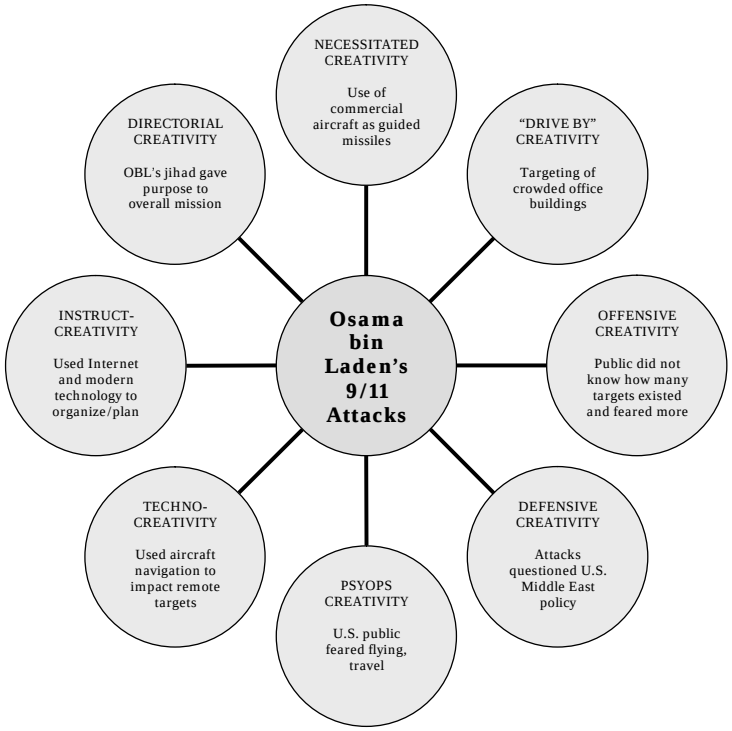


Figure 1. How the 9/11 Attacks Followed Creative Convention.

miserably. It speaks of cultivating the "hearts and minds" of target audiences yet fails to understand the basic concerns of such indigenous peoples.

Whether hailing from the plains of Equatorial Africa or the American Midwest, the average person considers very little outside of placing food on the table or a roof over his or her children's heads. To corral the attention of such individuals, either one of two approaches needs to be effected: (1) The people need to be convinced that the status quo is under imminent attack; or (2) they need to be convinced that the status quo is unattractive to suit their desires and needs. Whichever goal represents the challenge, its successful implementation rests largely upon the talents and laurels of creative personalities, for such citizens need to be *inspired* into a particular course of action instead of merely being persuaded through simple argument alone.

The United States traditionally assumes the first task – that of convincing its target audience that someone else is trying to destroy its culture or its sovereignty. Whether it was Nazi Germany, Communist Russia, or most recently Islamic jihadists, this approach often falls upon deaf ears. In this kind of atmosphere, only tragedy galvanizes the otherwise apathetic population of America. In contrast, foreign despots and rogue organizations often flourish during periods of domestic crisis – which may or may not have been initiated by their supporters – for which a brighter future represents *everything* to their constituents. Adolf Hitler extolled the merits of a thousand-year Reich, Che Guevara condemned the excesses of Western capitalism, and modern Islamic jihadists have orchestrated a powerful devotion through intoxicating interpretations of "Allah's Will" and lustful visions of Paradise.

Each of the above examples used creative manipulation of both global history and local legend to shower indigenous peoples with "heroes" that needed emulation. In the case of Che Guevara, for instance, post mortem popular marketing of his exploits served more to elevate his grandeur than did battlefield competence. What results from these choices is an eternal battle between arguments of "*It's a horrible idea for you to change your ways…*" and "*Brother, have I got something great in store for you!*"

Where the United States, specifically, loses in this contest is through believing that "the American Dream" can be transplanted *anywhere* – as long as sufficient effort is applied. American politicians continually fail to grasp that their particular system of beliefs is predicated upon individual acceptance and responsibility, i.e., that capital success remains a very individualistic phenomenon that runs against the grain in a society, such as that which is prevalent within the Middle East, where the masses are more important than the mere individual. In such an environment, authorities cannot address the concerns of singular families and expect to be successful in commandeering the culture as a whole.

HAVE GUN, WILL NOT NEGOTIATE

Brute strength represents the one commodity that *all* humans can fully appreciate. Few like to be counted among the weak or disadvantaged and fewer still fail to understand the primal options of survival or extinction. The "shot heard around the world" was, after all, fired from a weapon, even though it eventually heralded in the most individual-appreciative constitution in human history.

In Third World nations, particularly those surrounding the Middle East, individual liberties are nearly unheard of. Compounding the issue remains the fact that the religion of choice, Islam, mandates strict redistribution of wealth as blanket social policy. This contrasts sharply with Christianity, which permits the individual of substance to bear personal responsibility for his or her own charity and leads to appreciation of the problems associated with inspiring individuals within xenophobic Middle Eastern cultures. Governments cannot simply apply "hearts and minds" campaigns here without addressing the plural.

So how should Western governments address the issue? By exercising that underutilized force known as creative power. Every human person knows intimately the concept of brute strength, whether its appearance is set forth in military operations, local police patrols, or economic finesse. As much as modern military leaders tend to consider otherwise, the eternal relationship of creative reward and potential retribution cannot be divorced from one another. The world may occasionally remove a Saddam Hussein, for example, but preparations must be available to instill a surrogate until the culture percolating underneath finally simmers down.

As already discussed, people simply cannot change their lifestyles on the fly. They must feel, without undue concerns, that the future which awaits them is what they expected. The jihadists excel at this because Islam's version of a future – as religiously perverted as it appears to the West – offers little adaptation over that which most Middle Eastern residents endured for millennia. An Islamist Iraq, therefore, represents nothing more than a Saddamist Iraq did, with only the principal opportunists changed. An American-inspired democracy remains fully alien to those bred in a culture where the sword is mightier than the pen and religion filters into every aspect of existence. To compensate for this, Western military intelligence operations must take into consideration that their primary offensive function is not necessarily to control the population but to persuade it.

When confronted between two clear options, a citizen realizes but two distinct routes to take. He or she must follow defined concepts such as good or evil, Islam or democracy, freedom or subterfuge. Western political advocates tend to muddle the issue by granting the person in question freedom from choice, perhaps even offering the semblance of a third system from which to divert. The West's enemies are not so accommodating; they will challenge the individual to choose between either their forces or their "enemies." In this context, the decision remains a relatively easy one to make. They tend to accept the choice given to them, especially if the alternative is even more alien to their culture. The West, therefore, requires matching wits with its adversaries and removing the ambiguities associated with choice.

"YOU ARE EITHER WITH US OR…"

When an invading force arrives in virgin territory, it endeavors to conquer such "hearts and minds" of the local population. It illuminates the precise "reason" that it is there. When Chinggis Khan spoke to the people of Bukhara, he told his audience that he represented "the punishment of God."[26] Conversely, when the United States typically arrives on the scene, its leaders tell the population that Americans are there to instill a sense of freedom and liberty in them. In a culture bred on filial responsibility and divine destiny, who would they listen to? The Islamists perverting the Middle East simply adopted the role of Chinggis Khan and excuse every terror, crime, and blasphemy at their disposal as part of a master plan for divine retribution. America requires placing an end to this, enforcing upon indigenous populations the fact that the *only* difference between Western allies and that of the terrorist groups remains that America tends to treat its friends better.

U.S. Intelligence operations must convince these populations that Americans are just as decisive as the enemy but also able to shed some compassion upon them if inclined to do so. It needs to balance this potentiality with the fear that exists when the indigenous population believes that Americans have their homes bugged, their cousins turned, and their friends watching their every move. Neighborhoods must be diced into blocks and then homes and every suspicious person or vehicle transiting each "cell" scrutinized for purpose.

America also needs to address the issue of economic support and use this powerful tool as payment for friendship and not simply dole it out as a bribe. People who aid in providing intelligence must be compensated for generously, and those who do not aid in collecting information should not receive any support whatsoever. Military forces must, before considering any further action, convince an occupied population that it remains their

responsibility that the invaders had to arrive in the first place.

The West can, beyond a reasonable doubt, showcase the merits of free capital enterprise. The terrorists, in comparison, cannot. Military advisors can saturate a culture with images, videos, and testimony as to which system has the wherewithal for personal success. Sadly, the West usually does not. It long since divorced tactical military operations from the creative acquisition of primal intelligence. Through limits placed upon engagement, diplomacy as a means instead of an end, and political correctness as virtual law, U.S. forces cannot win first and spout questions later. War requires literally shocking a culture into choosing sides and this entails combining creative manipulation with a show of decisive power. Commanders therefore choose for them their beliefs and get them to thank everyone for it. An indigenous culture thus desires to become America's ally for fear of the alternative.

Historically, this has always been the case among the oppressed. Chicagoans of the early 20th century often sided with Alfonso Capone rather than inform on the gangster. Millions of Germans ignored the recognizable horrors of the "Final Solution" lest they draw the ire of Gestapo agents. At least one captain burned his vessel's lifeboats to prevent desertion. In American military parlance, however, such actions approach, if not define, tyranny. Yet, militaries are not democracies. Nor should they be. A military's first function is to impart decisive victory on behalf of its nation. Contributing to this "decisive victory" on behalf of an aggressive/defensive nation remain the allies which its leaders cultivate through creative enticement.

"VOODOO INTELLIGENCE" AND POLITICAL HYPERSENSITIVITY

In these Third World environments, where conflicts often simmer for decades, actionable intelligence remains at a premium. Often, decisions on who to attack, who to attract, and even how to react involve imposing Western-style politics upon medieval aspirants. This remains exceedingly difficult within regions where even monies are transferred via *hawala* practices. It remains an indiscriminate world in which beliefs flow through an interminable sea of thoughts, suggestions, and threats.

Deciphering intelligence from such sources whose entire existence rests within this commotion remains nearly impossible for Western analysts and operatives whose exposure to the environment often reflects a tour-based commitment at best. Compounding the problem is American and Western fascination with documentation (see Figure 2).[27] Such enchantment with "official-looking papers" merely represents a subconscious desire for self-

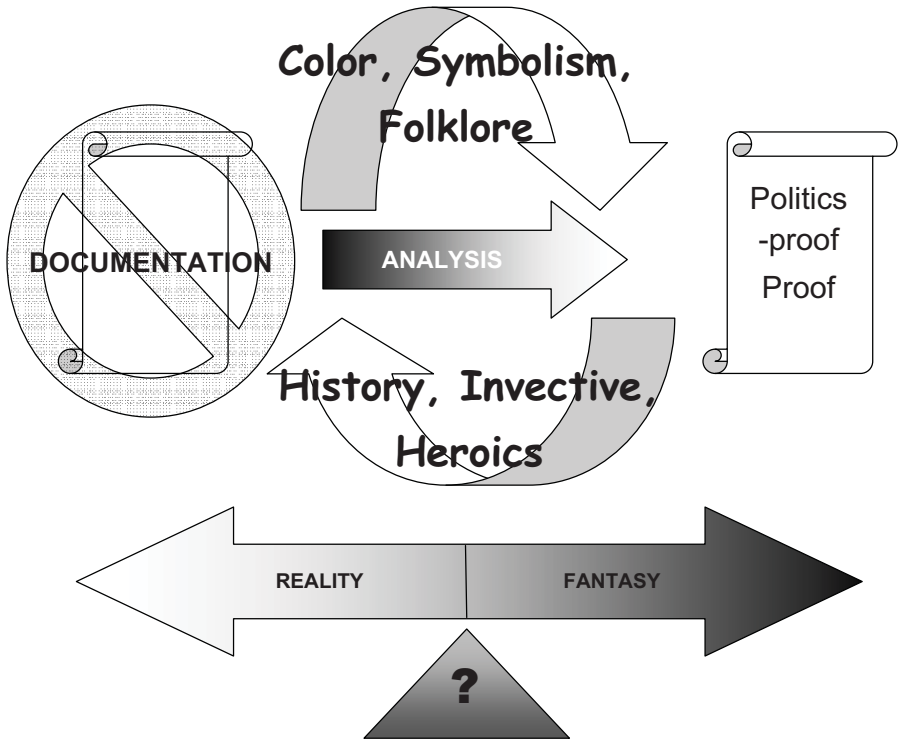


Figure 2. The World of "Voodoo" Intelligence.

preservation. Intelligence analysts, operatives, and even consumers can redirect the blame for failure upon inanimate objects – the specific document in question.

This remains problematic when the intelligence is culled from a "flood of genuine leaks, rumors, and bit and pieces of real significance."[28] More damage occurs when the intelligence gathered comes via third-party linguists and interpreters.

Foreign-trained interpreters possess neither the dialect nor the idiosyncrasies of indigenous populations, despite best effort attempts to consume the local flavor. Nor do domestic analysts, operatives, and political clients always interpret the "facts" of information as defined by such indigenous peoples. Much remains highly biased because of personal stereotypes, political correctness, and ignorance of regional perspectives (**see Table 2**).

Confusion as to interpretation illuminates the duality of creative behavior. It remains both a tool to confront intelligence as well as a weapon to expedite countermeasures.

Fortunately, there remain three broad personality types to distinguish personal characteristics from:

Political Personality Subtype: A political personality thrives on the merits and opportunities of public service. He or she generally favors government solutions to crises and more often than not reflects a conciliatory mannerism toward other political personalities, the media, or the nation. Intelligence gained from political sources remains highly suspect because of this nature to adjust toward broader audiences.

Historical Truth	Regional Faith	Secular/America/West
Muhammad ibn Abdallah personally led 27 military campaigns to establish his new faith.	Islam must pervade economics, politics, and warfare. Only when the world submits, can there be peace.	Islam is a religion of peace and tolerance. Muslims worship the same God as Jews and Christians.
There were no differences between Nazis and Soviet Communists	National Socialists and Soviet Communists were nationalist heroes.	Soviet Communists were "left-wing" and Nazis were "right-wing" politically.
The U.S. First Amendment protects religious practice.	"*Congress* shall make no law" interfering with religion.	*Government* shall make no law permitting religiosity in public.
The U.S. Second Amendment protects firearm ownership.	"The right of the people to keep and bear Arms shall not be infringed."	Founding fathers wanted only to protect hunting.
Intelligence comes from all sources.	"Tell 'X' what I have to say…"	It remains meaningless unless you can prove it beyond a reasonable doubt.
Jihadists embark upon war to satisfy their destiny.	Paradise is guaranteed only for those who die for Allah.	Western foreign policy is to blame for Islamic terrorism.
Education, regardless of source, remains invaluable.	"I learn, I remember, and therefore I know."	"I was taught, tested, and therefore I know."

Table 2. Representative Perspectives of Indigenous Interpretation.

Opportunistic Personality Subtype: An opportunist thrives upon return on investment, whether that enticement involves financial, educational, or career efforts. He or she generally favors free market capitalism owing to its value-added effects for individualism. Intelligence gained from opportunistic sources remains suspect because of the inherent nature of such personalities to derive "profit" from effort.

Militant Personality Subtype: A militant personality thrives upon competition as enforced through faith, ideology, and/or patriotism. He or she generally favors challenging situations, advancement, and camaraderie. Intelligence gained from militant personalities might be suspect depending upon their training, fanaticism, and loyalty to the organization/belief they serve.

Obviously, few individuals remain adherent to either of the above three personality types exclusively. Regardless, the underlying subtype presents itself with little effort on the part of the analyst (see Table 3). From this baseline perspective, the target individual's thoughts and actions present themselves. This baseline serves to characterize the individual's personality whether the "militant" remains employed within the media or the "politician" within academia.

Political Personality Subtype:

Personality Assessment: *Observed or Perceived Behavior*

- Public interaction _____
- Media attraction _____
- Education Background _____
- Languages _____
- Family/Friends/Associates _____
- Faith/Patriotism _____
- Hobbies/Leisure Activities _____

Intent of Political Personality

1. To seek office? Yes No which? _____
2. To serve constituency? Yes No how? _____
3. To gain prestige? Yes No why? _____

Ideology: _____
Social welfare considerations : _____
National defense considerations: _____
Does target personality's background/lifestyle match his or her ambitions and statements _____
_____

Opportunist Personality Subtype:

Personality Assessment: *Observed or Perceived Behavior*

- Public record _____
- Media attraction _____
- Education Background _____
- Languages _____
- Family/Friends/Associates _____
- Faith/Patriotism _____
- Hobbies/Leisure Activities _____

Intent of Opportunistic Personality

1. *To seek profit?* *Yes* *No* *value?* _____
2. *To seek power?* *Yes* *No* *how?* _____
3. *To gain prestige?* *Yes* *No* *why?* _____

Ideology: _____
Social welfare considerations : _____
Capital enterprise considerations: _____
Does target personality's background/lifestyle match his or her ambitions and statements _____
_____

Militant Personality Subtype:

Personality Assessment: *Observed or Perceived Behavior*

- Public record _____
- Family Background _____
- Education Background _____
- Nationality/Ethnicity _____
- Family/Friends/Associates _____
- Faith/Patriotism _____
- Hobbies/Leisure Activities _____

Intent of Militant Personality

1. To seek power? Yes No how? _____
2. To seek glory? Yes No why? _____
3. To serve nation? Yes No when? _____

Ideology: _____
Social servitude considerations : _____
National defense considerations: _____
Does target personality's background/lifestyle match his or her ambitions and statements _____
_____

Table 3. Distinguishing Personalities.

This capability permits the intelligence professional to isolate faked data and determine its reason for falsification, as well as to "play scraps into patterns."[1] Such curiosity, pattern recognition, interest in people, skepticism, patience, and nerve benefit counterintelligence agents too, for defense and offense remain equal parts of battle.[2]

Where politics, specifically, enters into the fray is when national leaders fail to grasp either the baseline personality of the subject or how the other two characteristics affect their motives. This remains exceptionally well illustrated within the battle against Islamic jihadists; Western politicians consistently fail to grasp the significance of the underlying doctrine as they seek to appease the population. They trend toward dismissing the founder's brutality and aggressiveness while harboring that the "majority" represents adherence. In reality, it often remains the *minority* which remains faithful to a particular ideology or religion.

CONCLUSIONS

When Titus approached Jerusalem in 70 A.D., the Roman's arrival infused the 18-month siege of the city with "exceptional speed and vigour [sic]," and in doing so took the Jewish population completely by surprise.[3] Whatever the military commander's reflection upon creative endeavor, the Jews ultimately remembered him as the "wicked Titus who blasphemed and insulted Heaven."[4] Like Chinggis Khan during 1220 A.D., Titus cared less about infringing upon people's sensibilities. His army gained invaluable intelligence about his enemy (including that of atrocities which even offended Roman sensibilities) and acted upon it with creative disregard for standard procedures.

Both the Roman Titus and the Mongol Khan possessed what the ancient Japanese ninjas referred to as *saiminjutsu* – a warrior's version of hypnosis.[5] While it remains improbable that either Titus or Chinggis Khan tried to hypnotize individuals, their subsequent tactics did captivate their enemies and, in the case of the Mongol, permitted him to stand within a crowded mosque and declare to all Muslims that the "infidel" represented God's punishment for their sins – shock creativity at its best.

In the modern era, a significant gulf rests between intelligence gathering and actionable response. More often than not, information gathered within the field is transmitted back to national headquarters and recycled consistently before a decision is made to conduct a raid, ambush, assassination, or reconnaissance mission. The advent of modern, high-speed communications technology merely shortens the period of time between approved collection and application. It does not eliminate the barriers to response. Technology simply becomes an *nth*-generation development of political oversight upon the battlefield.

What remains is an intelligence/special operations community that serves little but to bureaucratize primal warfare for political gain.[6] Any delay between collection and application produces sloppy intelligence and "[s]loppy intelligence targeting kills a great many people, kills them needlessly."[7] Needless deaths compound the ability to target productive kills and disrupt a nation's support from its civilian population.

To correct this discrepancy, several adjustments on the part of Western political and military leadership require attention:

- *Place combat decisions as close to the scene of battle as possible*. Those being shot at certainly merit the ability to return fire. However, Predator drone operators, for instance, must be granted full authority to launch Hellfire missiles as soon as the threat warrants. Deferring to higher authority merely grants the enemy quarter, and denying such adversaries any quarter is what active combat operations are all about;

- *Eliminate politics from active combat operations*. It remains one thing for politicians to legislate military protocol, quite another for legislators and public leaders to redefine war. Western politicians and military commanders must reflect consciously upon the words of General William Tecumseh Sherman: "*If the people raise a great howl against my barbarity and cruelty, I will answer that war is war, and not popularity seeking*";

- *Psychological warfare operations must detach themselves from simple "hearts and minds" campaigns and refocus energies upon applying "absolute power" against the enemy*. People reared upon millennia of tribal politics and Bedouin warfare will not quickly succumb to expectations of democracy and porcelain bidets. As Iraq proved, quickly removing the lid on a simmering pot will likely flash into a chaotic situation beyond the capability to respond to the crisis from those on the ground;

- *Engage creativity within special operations forces*. Of all military units, those representing special operations forces (SOF) represent the best trained and recruited for creative

intelligence, courage, and physical fitness – traits that British Major General J.F.C. Fuller once found necessary for all great generals. SOF operatives must not be considered "launch and forget" units, but their attachment to general officers must reflect upon their own experiences and needs, not the other way around;

- *Cease "popularity seeking" during periods of conflict*. The role of a nation's intelligence service remains to defend that country and the role of its military remains to defeat any and all adversaries. Intelligence collection, therefore, requires all assets, methods, and resources while military action must account for "any means necessary." War is meant to *offend*, not patronize.

With the conclusion of the Second World War, warfare and conflict took upon itself a decidedly lackadaisical nature, particularly within the West. Unconditional surrender no longer represented the gratuitous buzzword of Washington, London, or Paris. Instead, phrases such as "Police Action," "Counterinsurgency Operations," and now, apparently, "Manmade Contingencies" earned their way into political favor.

For a society dutifully tuned to *American Idol* and *Dancing with the Stars*, perhaps such terms persist to avoid disrupting their evening lattes as they eagerly wait out who will be booted off the latest episode of *Survivor*. Unfortunately, politicians eager to win the "latte vote" fail to comprehend the further words of General Sherman: "*War is cruelty. There is no use trying to reform it. The crueler it is, the sooner it will be over*."

To end wars quickly, U.S. and other Western officials need to create an ever-lasting sense of shock upon their enemies, sufficient to disrupt their plans and actions until democracies prevail. To accomplish this, both intelligence agencies and military commands must endorse creative license to its fullest and infuse the innovative human mind with its primal instinct for survival. Only when adversaries are literally shocked into submission are they receptive to diplomacy. And not a moment before…

Notes

[1] Balor, Paul, 1988, *Manual of the Mercenary Soldier*, Paladin Press, p. 216.
[2] Peters, Ralph, *When Muslim armies won: lessons from yesteryear's jihadi victories*, *The Armed Forces Journal*, September, 2007, pp. 40-41.
[3] Grossman, David A., 1993, "Defeating the Enemy's Will: The Psychological Foundations of Maneuver Warfare," in *Maneuver Warfare: An Anthology*, edited by Richard D. Hooker, Jr., Presidio Press, p. 146.
[4] Tucker, David, "Fighting Barbarians," *Parameters*, Summer 1998, pp. 69-70.
[5] Balor, Paul, 1988, *Manual of the Mercenary Soldier*, Paladin Press, p. 225.
[6] Scales, Robert H., "Urban Warfare: A Soldier's View," *Military Review*, January-February 2005, p. 11.
[7] May, Timothy, 2007, *The Mongol Art of War*, Westholme, p. 69.
[8] Tucker, David, "Fighting Barbarians," *Parameters*, Summer 1998, p. 70.
[9] Gentile, Gian, "Eating Soup with a Spoon," *Armed Forces Journal*, September 2007, p. 33.
[10] Vego, Milan, "The NCW Illusion," *Armed Forces Journal*,. January 2007, p. 39.
[11] Scales, Robert H., "Urban Warfare: A Soldier's View," *Military Review*, January-February 2005, p. 13.
[12] Godlewski, R.J., *Implementing Innovative Leadership in an Era of Catastrophic Weapons*, http://www.rjgodlewski.com/ImplementingInnovativeLeadershipByRJGodlewski.pdf, 2008, p. 5.
[13] Godlewski, R.J., *Surgical Warfare: An Impediment to Conflict Resolution?* http://www.rjgodlewski.com/SurgicalWarfare.html, 2003.
[14] Tucker, David, "Fighting Barbarians," *Parameters*, Summer 1998, p. 69.
[15] Scales, Robert H., "Urban Warfare: A Soldier's View," *Military Review*, January-February 2005, p. 15.
[16] Ibid.
[17] Ibid.
[18] Ibid., p. 15.
[19] Carl Gustav von Rosen's use of "weaponized" light private airplanes as counterinsurgency aircraft is being replicated today with the use of business and commercial aircraft as intelligence, surveillance, and reconnaissance aircraft necessitated from similar needs.
[20] Suicide bombings epitomize "drive by" incidents in urban America as they represent attacks without notice and leave very little in which to retaliate against.
[21] "Shock and Awe" maintained pressure because the Iraqis, the media, and even the rest of the world were continually held in expectation of what "has yet to come."
[22] MacArthur's landings at Inchon not only caught the North Koreans unprepared, they had an almost immediate result of reducing strain upon the beleaguered Pusan Perimeter.
[23] Hadley, Arthur T., 1993, "Maneuver Warfare and the Art of Deception," *Maneuver Warfare: An Anthology*, edited by Richard D. Hooker, Jr., Presidio Press, pp. 364-365.
[24] This is where faked videos, tweaked images, and fabricated radio broadcasts come into play. Welles used the airwaves and expectations of popular music to convince the public that the planet was under attack and, later, Iran superimposed multiple images to convince Western media that several missile firings had taken place.
[25] Kennedy's statement, uttered before the nation had even achieved manned orbit, galvanized an entire country. Later, following his assassination, the goal became one of patriotic duty and went so far as to divert attention away from the escalating conflict in Vietnam.
[26] May, Timothy, 2007, *The Mongol Art of War*, Westholme Publishing, p. 1.

[27] Balor, Paul, 1988, *Manual of the Mercenary Soldier*, Paladin Press, p. 228.
[28] Ibid.
[29] Ibid., p. 229.
[30] Johnson, William R., 2009, *Thwarting Enemies at Home and Abroad*, Georgetown University Press, pp. 7-12.
[31] Goodman, Martin, 2007, *Rome and Jerusalem: The Clash of Ancient Civilizations*, Alfred A. Knopf, p. 17.
[32] Ibid., p. 479.
[33] Hayes, Stephen K., 1981, *The Ninja and the Secret Fighting Art*, Charles E. Tuttle Company, p. 132.
[34] Baer, Robert, 2010, "A Dagger to the CIA," in *GQ Politics* (April), http://www.gq.com/news-politics/politics/201004/dagger-to-the-cia.
[35] Balor, Paul, 1988, *Manual of the Mercenary Soldier*, Paladin Press, p. 230.

R.J. Godlewski (pronounced GOD-LESS-KEY) is an independent counterterrorism consultant; the director of the private International Nuclear Emergency Response Team (INERT); and the author of several novels, commentaries, and professional articles. He is also the author and architect of the Internet-based Independent Counterterrorist training program. He is currently completing his BA in Intelligence Studies at American Military University with a concentration in Middle East terrorism and holds an undergraduate certificate in Explosive Ordnance Disposal. He intends to begin a master's program in Asymmetrical Warfare during late 2011. Mr. Godlewski is a member of NMIA, as well as a veteran of both the U.S. Navy and Navy Reserve. His article, "Human Intelligence: Perceiving an Enemy's Thoughts," appeared in the Fall 2009 issue of AIJ. *The author welcomes questions or comments about his work; he can be contacted at rjgodlewski@rjgodlewski.com.*

Intelligence Community Assessment:
Generational Differences in Workplace Motivation

by Dr. James McGinley, Tim Weese, Jennifer Thompson, and Kevin Leahy

OVERVIEW

An exploratory qualitative study was conducted to achieve consensus among Generation X and Generation Y employees working in a U.S. Department of Defense intelligence activity with regard to workplace motivations and reward and recognition preferences. The research goal was to make a practical contribution by considering a comparative, empirically-based approach to understanding workplace motivation within the Intelligence Community. Results indicate that Generation X and Generation Y workforce cohorts have a dominant preference for intrinsic motivation. Despite concerns over cultural differences, these cohorts reported several shared motivational as well as reward and recognition preferences. A surprise finding of this study was the preference for verbal praise by both Generation X and Generation Y employees. These results may challenge previous findings that workforce cohorts are culturally dissimilar and may encourage a reexamination of the role of organizational leadership when designing transformational initiatives.

INTRODUCTION

In the course of its history the United States Intelligence Community (IC) has undergone many reforms. Contemporary reforms have emphasized both organizational and workforce initiatives. Yet, there is increasing concern that transformational initiatives must be considered in the context of changing workforce demographics (Office of the Director of National Intelligence, 2006). Changing workforce characteristics may impact the effectiveness of pay, reward, and recognition systems if demographic-based generational differences in the workforce translate into new norms of expectation and motivation. Research indicates that generational differences may impact workplace motivation (Bolton, 2010) but its impact in the IC workforce remains to be fully assessed. This article addresses the research need to conduct an IC workforce assessment that can empirically categorize generational differences in workplace motivation.

Reform initiatives within the IC and emergent demographic shifts have created a need to reexamine the foundations, and potential differences, of workforce motivation. For example, the Office of the Director of National Intelligence's (ODNI) Analytic Transformation initiative seeks to shift long-standing intelligence operations in the direction of greater collaboration (ODNI, 2008). Such an emphasis on workplace production and interpersonal environments may benefit from a greater understanding of the motivational needs of employees. In addition, the Defense Civilian Intelligence Personnel System (DCIPS) initiative to move the IC workforce to a pay for performance system could be jeopardized by poor employee confidence (U.S. Government Accountability Office, 2009). The decision to refocus the DCIPS program is likely to bring new attention to the relationship between performance incentives and employee motivational needs. Concurrent with these initiatives is the awareness that workforce demographics are changing as the current generation of leaders and analysts is replaced by the next workforce cohort (ODNI, 2008). The goal of this pilot study was to attempt to make a practical contribution to the ongoing dialogue by considering a comparative, empirically-based approach to understanding workplace motivation within the Intelligence Community.

BACKGROUND

The events of September 11, 2001, provided a new sense of urgency to long-standing concerns over the need to make improvements within the U.S. Intelligence Community. The current research examined convergent trends in reform initiatives and workplace demographics through the theoretical lens of employee motivational needs.

Reform and Strategic Alignment

The 9/11 attacks resulted in the development of a broad governmental reform agenda. These reforms consisted of both organizational and workforce initiatives. For example, the 9/11 Commission recommended several transformational organizational changes for intelligence

such as the establishment of a National Counterterrorism Center (NCTC) and the unification of the IC under a new National Intelligence Director (9/11 Commission, n.d.). Subsequently, the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) established both the NCTC and the Office of the Director of National Intelligence (Best, 2010). In the spirit of reform, ODNI began developing a series of analytic transformation initiatives designed to increase information sharing and integration, such as the establishment of an IC badge interoperability program, a joint duty program, and the introduction of collaborative efforts such as Intellipedia, A-Space, the Summer Hard Problem Program, and the Library of National Intelligence (Best, 2010; ODNI, 2008). Concurrent with functionally-focused initiatives such as these is concern that there is also a need to strategically align workforce initiatives, including measures to address the impact of changing workforce demographics, within an integrated approach (ODNI, 2006).

Shifting Workforce Demographics

Changing workforce demographics have become of increasing concern within the Intelligence Community. Of particular concern is an imbalance within the IC workforce in which there exists a disproportionate concentration of post-9/11 employees on the one hand and a large pool of retirement-eligible employees on the other (ODNI, 2006). This imbalance is the result of tight budgets and constrained hiring during the 1990s, which created a gap in workforce accession, and a resurgent wave of post-9/11 new hires (ODNI, 2006). The Office of the Director of National Intelligence has specifically expressed concern over the "greening" of the workforce and the need to maintain a sense of urgency in transformational initiatives (ODNI, 2008).

However, while concerns have been focused on the youngest portion of the U.S. workforce, the global recession has also had an unexpected impact on the "grayer" end of the total national workforce. According to the Bureau of Labor Statistics (BLS), those aged 55 and older made up 18.7 percent of the workforce and that percentage is expected to grow to 22.7 percent by 2016. Overall, it is projected that the U.S. workforce will increase by 12.8 million workers from 2006 to 2016. The number of workers aged 16 to 24 will decrease by 1.5 million, the number aged 25 to 54 will increase by 2.5 million, and the number aged 55 and older will increase by 11.9 million (see Pew Research Center, 2009). However, a dramatic generational transition is anticipated as the oldest workforce cohort retires (Gilburg, 2007).

There is a perceived need within the IC to recalibrate its human capital system to accommodate the needs of a new workforce generation that may possess different norms of work and interaction than the previous generation.

It is not surprising that the ODNI has identified shifting workplace demographics as a key external condition which can shape IC transformation (ODNI, 2008). The ODNI has specifically expressed a need to win the war for talent in the competitive labor market by both recruiting and retaining the best and brightest candidates (ODNI, 2006). This recruiting challenge may also be shaped by perceptions that new workforce cohorts possess generational differences. There is a perceived need within the IC to recalibrate its human capital system to accommodate the needs of a new workforce generation that may possess different norms of work and interaction than the previous generation (ODNI, 2006). The present comparative study specifically examined that concern by conducting an empirical assessment of motivational needs.

Generational Cohorts

The U.S. workforce consists of at least four generations coexisting within the workplace. These generations are categorized by year of birth cohorts. From oldest to youngest, they may be labeled as Seniors (born 1900-1945), Baby Boomers (1946-1964), Generation X (1965-1980), and Generation Y (1981-2000) (Bolton, 2010). However, these titles and age ranges are not definitive. For example, the Seniors cohort may also be referred to as Traditionalists or Veterans, Generation X as Xers, and Generation Y as Millennials or Nexters (Bolton, 2010; Legault, 2002). In addition, the age ranges may vary slightly with the Baby Boomer cohort alternatively described as 1944-1960 and Generation X as 1961-1980 (Legault, 2002). Because one purpose of this study is to inform transformational discussions, it selected to focus on Generation X (defined as 1960-1979) and Generation Y (defined as 1980-2000), since these cohorts will begin career transitions into mid- and senior-level management positions. Therefore, it would be reasonable for policies being developed now to consider their impending rise in the workforce.

Age-based workforce cohorts are of importance because they may potentially embody different value systems and attributes. Before a full understanding of the IC workforce can be attained, it is helpful to first understand the attributes of the general workforce from which it is drawn. Although research continues to explore their differences, Figure 1 provides a broad conceptualization of attribute

differences between the Generation X and Generation Y cohorts (see Crumpacker & Crumpacker, 2007).

	Generation X	Generation Y
Work ethic	Task-oriented	Multi-tasking
	Self-reliant	Group-oriented
	Independent	Explain why
Communication	Direct	Email/voice mail
	As needed	Instant messaging
Feedback	Direct - "Tell me how I am doing."	Instantaneous
		Seek approval/praise
Stereotype	Cynical	Spoiled
	Less open to change	Open to change

Figure 1. **Comparative Attributes of Generation X and Generation Y**

Generation X is described as being a technologically-savvy generation, pragmatic, and competent; its members are efficient at managing themselves to get the job done. They tend to be free agents, frequently distrusting corporate motives; most have received very little training, development, or mentoring in the workplace, and hence are adept at learning on the fly (Gilburg, 2007). Family is a priority to Generation X members. They put family first over their careers and often come in and out of the workforce to meet family needs (Williams, 2009). Other common descriptors of this generation are cynical, distrust of authority, self-sufficient, casual, and value quality of life. Key influences on this generation have been corporate downsizing, Nixon resignation and pardon, latchkey kids, legacy of Vietnam pullout, and the rapid growth of technology (Licata, 2010). Motivators of Generation X are freedom to do things their way or independence. Irritators can be described as clichés, authority figures, and formalities (Licata, 2010).

Generation Y is described as self-sufficient, hard-working, hopeful, relaxed gender roles, comfortable with diversity, value networks and groups, highly knowledgeable, and comfortable with technology. Key Influences for this generation have been school shootings/violence, the Challenger disaster, Gulf War, DESERT STORM, War on Terror, soccer moms/helicopter parents, and highly scheduled childhoods (Licata, 2010). Generation Y motivators seem to be work-home balance, working in teams, structure and supervision, feedback, understanding the details of why and how things are to be done, make a difference, and friendship in the workplace. Irritators for this cohort can be described as long/rigid working hours, inflexibility, and strictly independent/isolated work. They are fundamentally conservative in their lifestyle, with a dislike for ambiguity and risk (Williams, 2009).

Theoretical Foundations

The motivational theories of Maslow, Alderfer, and Herzberg include needs-based dimensions (Agarwal, 2010). Their theories include both extrinsic (external) and intrinsic (internal) sources of needs satisfaction. Maslow described a five-tiered hierarchy of needs which were ordered in precedence from physiological needs to self-actualization (Myers, 1995). Alderfer reduced Maslow's hierarchy from five to three factors, re-conceptualizing needs as related to existence, relatedness, and growth (Agarwal, 2010). Herzberg's two-factor approach characterized needs satisfaction as either motivation (intrinsic) or maintenance (extrinsic) factors (Baldonado & Spangenburg, 2009). The current study continues the exploration of internal and external dimensions by categorizing extrinsic and intrinsic motivational drivers within the IC workforce.

Intrinsic motivation is achieved when the activity itself provides pleasure and satisfaction (Vallerand et al., 1992). Intrinsic motivation can be expressed in several forms. One is the activity itself (e.g., attending a lecture about a subject in which one is interested), meeting standards for their own sake (e.g., ethical standards or production standards), or accomplishing a personal or professional goal (Frey & Osterloh, 2002). On the other hand, extrinsic motivation refers to a wide range of activities that are engaged in not for their own sake but for the potential end state (Vallerand et al., 1992). Extrinsic rewards often take the form of tangible financial rewards (Thomas, 2009). In the context of workplace motivation, extrinsic rewards often relate to a need to satisfy non-work-related needs and work serves as a tool to satisfy those needs by the salary or tangible rewards it provides (Frey & Osterloh, 2002).

METHOD

In this exploratory qualitative study, the researchers sought consensus among employees working in a U.S. Department of Defense intelligence activity regarding workplace motivations. A modified Delphi method with two rounds of questionnaires was used, followed by a survey on preferences for current workplace reward and recognition options. The Delphi method is useful in conditions where consensus is sought and where the research goal is to distinguish and clarify perceived human motivations (Linstone & Turoff, 2002).

The goal of the present research was to establish employee preferences in two areas: workplace motivational needs and reward and recognition preferences. It was conducted in two rounds as a short survey questionnaire. In Round 1, participants ranked the top 5 preferred (1-5, most preferred to less preferred) workplace motivators based on the

Workplace Extrinsic and Intrinsic Motivation Scale (WEIMS) (Tremblay, Blanchard, Villeneuve, Taylor, & Pelletier, 2009). Participants were also provided with the opportunity to add additional motivators to the list and to provide comments. The WEIMS provides a list of 18 extrinsic and intrinsic workplace motivations (e.g., "Because it allows me to earn money" and "Because it has become a fundamental part of who I am") and has been found statistically sound for research use (Tremblay et al., 2009).

After consolidation of Round 1 results and comments, a Round 2 survey was conducted in which participants re-ranked their preferences for workplace motivators from the new consensus-based list. The Round 2 list included the original WEIMS components plus any new motivational preferences stated by participants during Round 1. Additionally, in order to provide an assessment of current workplace reward and recognition options, employees also concurrently completed a survey in each round in which they sorted available reward and recognition options (e.g., bonuses, time off awards, verbal praise, etc.) in preference order from 1 to 5 (most preferred to less preferred).

RESULTS

This exploratory study conducted a comparative assessment of civilian employees (n = 19) currently working in a U.S. Department of Defense intelligence activity. This sample size represented 16.4 percent of the total civilian participants available across all age cohorts. Participants included a non-probabilistic sample of individuals born between 1960 and 1980, referred to as Generation X (n = 10), and individuals born between 1980 and 2000, referred to as Generation Y (n = 9).

		Generation X	Generation Y
Employment status	Supervisory	4	2
	Non-supervisory	6	7
IC experience (years)	Mean	14.8	4.3
Gender	Male	8	6
	Female	2	3
Age (years)	Mean	42.3	27.2

***Figure 2*. Descriptive Statistics for Generation X and Generation Y Employees**

Employment status included supervisory (Generation X, n = 4; Generation Y, n = 2) and non-supervisory (Generation X, n = 6; Generation Y, n = 7) personnel. Total work experience within the IC for Generation X was Mean = 14.8 years, and for Generation Y Mean = 4.3. The sample included both male (Generation X, n = 8; Generation Y, n = 6) and female (Generation X, n = 2; Generation Y, n = 3) participants. Ages for Generation X were Mean = 42.3, and for Generation Y Mean = 27.2. See Figure 2 for a summary of Generation X and Generation Y descriptive statistics.

Workplace Motivations

In Round 1 of this study, participants ranked 18 workplace motivators from the Workplace Extrinsic and Intrinsic Motivation Scale in order of preference. This scale asks respondents to assess the reasons why they are involved in their current work. In addition, they were provided the opportunity to list any additional workplace motivators that they considered important. For Generation X, respondents provided two additional workplace motivators ("Because I want to make a difference"; "Because it allows me to spend more time with my family"). For Generation Y, respondents provided eight additional workplace motivators (e.g., "Because my work contributes to something greater"; "Because I am connected to my work environment and enjoy being at work").

In Round 2, participants were provided the newly expanded list and were asked to re-rank all the items. The result was a preference list of the top five workplace motivators for each workforce generation (see Figure 3). This iterative, consensus process resulted in one new item not listed on the WEIMS list ("Because I want to make a difference") to enter into consideration by Generation X and be ranked as a preference. It also resulted in one new item not listed on the WEIMS list [For unique experiences (e.g., travel, work with other nations, etc.)] to enter into consideration by Generation Y and be ranked as a preference. It is interesting to note that the top two motivational preferences are both intrinsic and are shared by both workforce generations.

Reward and Recognition Preferences

In Round 1 of this study, participants also ranked 18 workplace reward and recognition options derived from current organizational policies in order of preference. In addition, they were provided the opportunity to list any other additional workplace reward and recognition preferences that they considered important. For Generation X, respondents provided two additional reward and recognition options (Recognition from peers/co-workers; Verbal recognition from Headquarters). For Generation Y,

	Generation X		Generation Y	
Rank	Item	Type	Item	Type
1	For the satisfaction I experience from taking on interesting challenges.	Intrinsic	Because I derive much pleasure from learning new things.	Intrinsic
2	Because I derive much pleasure from learning new things.	Intrinsic	For the satisfaction I experience from taking on interesting challenges.	Intrinsic
3	Because I want to make a difference.	Intrinsic	For the income it provides me.	Extrinsic
4	For the satisfaction I experience when I am successful at doing difficult tasks.	Intrinsic	Because this type of work provides me with security.	Extrinsic
5	Because it has become a fundamental part of who I am.	Intrinsic	For unique experiences (e.g., travel, work with other nations, etc.).	Intrinsic

Figure 3. **Generational Workplace Motivation Preferences**

respondents provided four additional reward and recognition options (e.g., Opportunity to do something I wouldn't be able to as a civilian; Enhanced reputation among colleagues).

In Round 2, participants were provided the newly expanded list and were asked to re-rank all the items. The result was a preference list of the top five workplace reward and recognition preferences for each workforce generation (see Figure 4). The iterative, consensus process used in the present study resulted in no new item not already listed on the Round 1 survey to be ranked as a preference.

Regarding Generation Y reward and recognition preferences, it is important to note that, although the preference for an end-of-year performance bonus ranked first in terms of the frequency in which it was included in the top five preferences, in no case was it ranked higher that 4 on a scale of 1-5. Yet, although the preference for verbal recognition from supervisor was ranked just lower based on frequency count, in no case did it receive a mark of lower that a 1 on a scale of 1-5. These results may indicate that, although extrinsic rewards are considered broadly important, there is a dominant preferential bias toward intrinsic rewards and recognition.

DISCUSSION

The IC maintains a concern over the impending generational shift in its workforce and the potential for a clash of workforce cultures to occur (ODNI, 2006). However, the results of this modest study indicate that it is likely that Generation X and Y workforce cohorts may, in fact, share several motivational preferences. For example, it is interesting to note that the top two motivational preferences (For the satisfaction I experience

	Generation X		Generation Y	
Rank	Item	Type	Item	Type
1	Verbal recognition from your supervisor.	Intrinsic	Verbal recognition from your supervisor.	Intrinsic
2	Recognition from peers or co-workers.	Intrinsic	End-of-year performance bonus.	Extrinsic
3	Verbal recognition from the unit Commander.	Intrinsic	Verbal recognition from your Division Head.	Intrinsic
4	End-of-year performance bonus.	Extrinsic	Verbal recognition from the unit Commander.	Intrinsic
5	Verbal recognition from your Division Head.	Intrinsic	Spot Award - monetary bonus.	Extrinsic

Figure 4. **Generational Reward and Recognition Preferences**

from taking on interesting challenges; Because I derive much pleasure from learning new things) are both intrinsic and are both shared by Generation X and Y workforce cohorts (see Figure 3). Research has indicated there may be other shared motivational dimensions across workforce generations, including a desire for respect, flexibility, fairness, and the opportunity to do interesting and rewarding work (Watt, 2010). These findings and the present study's results may challenge decision- and policy-makers within the IC to rethink perceptions of differences within the workforce and consider how to best take advantage of its shared motivational components.

The present study found that Generation X and Y reported a mixed preference for both intrinsic and extrinsic rewards and recognitions (see Figure 4). However, the present study did find a dominant, but not exclusive, preference for intrinsic motivation. These findings are generally supported by Herzberg's two-factor theory of motivation, which requires that both intrinsic and extrinsic factors be present at minimum levels. In this sense, the factors can be seen as parallels, not opposites (Bolton, 2010). Extrinsic rewards can be characterized as necessary but not sufficient. That is, the presence of extrinsic rewards is necessary to avoid worker dissatisfaction, but without being complemented by intrinsic rewards they are insufficient to achieve full worker satisfaction. Hence, there may be a need for reward systems to achieve a pragmatic and motivational balance.

In addition, a surprise finding of this study was the elevation of each of three verbal praises into the top five list of preferred forms of rewards and recognitions (see Figure 4). Although the specific rankings differed slightly, each generation categorized verbal recognition from supervisor, Division Head, and Unit Commander as important. It is revealing that Generation X and Y both reported that verbal praise from their immediate supervisor was the most preferred source of reward or recognition. This emphasis on the immediate organizational chain of command and personal leadership is striking. Leader-member exchange (LMX) theory describes role processes between leaders and subordinates. Research has established that verbal praise produces an increase in intrinsic motivation (Cameron & Pierce, 1994) and that favorable downward exchange relationships (i.e., leader to subordinate) are usually associated with higher satisfaction, stronger organizational commitment, and better subordinate performance (Yukl, 2002). The results of the present study may prompt a rethinking of the role that leadership serves and its reconsideration as a source of motivational reward for the workforce.

The Generation Y of today may become the Generation X of the future. This observation may indicate that transformational initiatives must be prepared to address a variety of age differences simultaneously.

The results of the present study may also encourage a re-conceptualization of differences in workforce generational cohorts. The current trend may be to see workforce cohorts as distinct and static; that is, they are likely to continue their current traits into the future. However, that may not be fully true. Over their lifespan, people face different normative challenges at various age levels in their lives (Erikson, 1959/1980). The present study's finding of a preference in Generation X for intrinsic motivation and a mixed preference in Generation Y for both intrinsic and extrinsic motivations may reflect the lifecycle challenges of their current chronological ages. For example, Generation Y's mixed motives may reflect their need to achieve both social and career goals common to all persons at their age. It may be possible that Generation Y will move toward the motivational pattern of Generation X as it matures in its life cycle (Jorgensen, 2003). That is, the Generation Y of today may become the Generation X of the future. This observation may indicate that transformational initiatives must be prepared to address a variety of age differences simultaneously, since differences may be tied to individual life cycle stage instead of generational cohort status.

LIMITATIONS AND FUTURE RESEARCH

A research objective of the present study was to validate the Delphi method as suitable for assessment of workplace motivational needs. Despite limitations of sample size in the present study, the Delphi method was able to define clear distinctions in motivational preferences. While the open comment component of the Delphi method was able to bring new preferences to light, this component of the study may be considered for expansion in a future study. That is, a future study may consider a combined approach, one that utilizes the Delphi method to achieve consensus and define preferences as well as a content analytic approach to more rigorously examine the thematic content of survey comments. It may be possible that nuanced observations on generational preferences may be discovered in participant commentary.

Of particular interest to future researchers may be the potential for additional similarities or differences to exist in preferred communication styles between workforce generations. A surprise finding of the present study was

that verbal praise was highly preferred by both Generation X and Generation Y cohorts. Since this finding appears to contradict previous research that supports generational differences in communication preferences (Crumpacker & Crumpacker, 2007; Hammill, 2005), this topic may be of further research interest.

CONCLUSION

The research goal of this exploratory study was to examine convergent trends in IC reform and workplace demographics through the theoretical lens of employee motivational needs. Its findings that some common motivational needs are shared across workforce cohorts may challenge a rethinking of the perception that divisive generational differences may exist within the workforce. Further, despite recent emphasis on pay for performance as a workforce management tool, it was found that intrinsic motivational needs and rewards are the dominant employee preferences. Since research results indicate that these are strongly based on direct employee and management communication, there may be a need for transformational initiatives to expand their focus from policy to include issues of workplace leadership.

References

Agarwal, A. (2010). Motivation and executive compensation. *IUP Journal of Corporate Governance, 9*(1/2), 27-46. Retrieved from ABI/INFORM Global. (Document ID: 1965392551).

Baldonado, A., & Spangenburg, J. (2009). Leadership and the future: Gen Y workers and two-factor theory. *Journal of American Academy of Business, 15*(1), 99-103. Retrieved from ABI/INFORM Global. (Document ID: 1771189841).

Best, R. (2010). *Intelligence reform after five years: The role of the Director of National Intelligence (DNI).* Report R41295. Congressional Research Service: Washington, DC. Retrieved from http://www.fas.org/sgp/crs/intel/R41295.pdf.

Bolton, S. (2010). *Career motivation theory: Generational differences and their impact on organizations*. (Doctoral dissertation, Walden University, 2010) (Publication No. AAT 3391445).

Cameron, J., & Pierce, W.D. (1994). Reinforcement, reward, and intrinsic motivation: A meta-analysis. *Review of Educational Research, 64*(3), 363-423.

Crumpacker, M., & Crumpacker, J. (2007). Succession planning and generational stereotypes: Should HR consider age-based values and attitudes a relevant factor or a passing fad? *Public Personnel Management, 36*(4), 349-369. Retrieved from ABI/INFORM Global. (Document ID: 1426327151).

Erikson, E. (1980). *Identity and the life cycle*. New York: W.W. Norton. (Original work published 1959).

Frey, B., & Osterloh, M. (Eds.). (2002). *Successful management by motivation: Balancing intrinsic and extrinsic incentives*. New York: Springer-Verlag.

GAO. (2009). *DOD civilian personnel: Intelligence personnel system incorporates safeguards, but opportunities exist for improvement*. GAO-10-134. U.S. Government Accountability Office: Washington, DC. Retrieved from http://www.gao.gov/products/GAO-10-134.

Gilburg, D. (2007, January 31). Generation X: Stepping up to the plate. *CIO*. Retrieved from http://www.cio.com/article/28475/Generation_X_Stepping_Up_to_the_Leadership_Plate.

Hammill, G. (2005, Winter/Spring). Mixing and managing four generations of employees. *FDU Magazine Online.* Retrieved from http://www.fdu.edu/newspubs/magazine/05ws/generations.htm.

Jorgensen, B. (2003). Baby Boomers, Generation X and Generation Y? Policy implications for defence forces in the modern era. *Foresight : the Journal of Futures Studies, Strategic Thinking and Policy, 5*(4), 41-49. Retrieved from ABI/INFORM Global. (Document ID: 452052391).

Legault, M. (2002). *Bringing people together: A study of generational diversity and organizational culture*. (Master's thesis, Royal Roads University, 2002). Retrieved from ABI/INFORM Global. (Publication No. AAT MQ70912).

Licata, P. (n.d.). *Boomers! GenX! GenY! Oh my! Work values across the generations*. Retrieved from http://www.njodn.org/Zipped_2010_PDFs/4_P_Licata.pdf.

Linstone, H.A., & Turoff, M. (2002). *The Delphi Method: Techniques and applications*. Reading, MA: Addison-Wesley.

Myers, D. (1995). *Psychology* (4th ed.). New York: Worth.

ODNI. (2006, June 22). *The US intelligence community's five year strategic human resource plan: An annex to the US national intelligence strategy*. Office of the Director of National Intelligence: Washington, DC. Retrieved from http://www.dni.gov/publications/DNIHumanCapitalStrategicPlan18October2006.pdf.

ODNI. (2008, September 1). *Analytic transformation: Unleashing the power of a community of analysts.* Office of the Director of National Intelligence: Washington, DC. Retrieved from http://odni.gov/content/AT_Digital%2020080923.pdf.

Pew Research Center. (2009, September 3). *America's changing workforce: Recession turns a graying office grayer*. Pew Research Center: Washington, DC. Retrieved from http://pewsocialtrends.org/pubs/742/americas-changing-work-force.

The 9/11 Commission Report. (n.d.). U.S. Government Printing Office: Washington, DC. Retrieved from http://www.gpoaccess.gov/911/pdf/fullreport.pdf.

Thomas, K.W. (2009). The four intrinsic rewards that drive employee engagement. *Ivey Business Journal Online*. Retrieved from ProQuest.

Tremblay, M., Blanchard, C., Villeneuve, M., Taylor, S., & Pelletier, L. (2009). Work Extrinsic and Intrinsic Motivation Scale: Its value for organizational psychology research. *Canadian Journal of Behavioural Science, 41*(4), 213-226.

Vallerand, R., Pelletier, L., Blais, M., Briere, N., Senecal, C., & Vallieres, E. (1992). The academic motivation scale: A measure of intrinsic, extrinsic, and motivation in education. *Educational and Psychological Measurement, 52*, 1003-1017.

Watt, D. (2010, March). Different generations, same objectives. *CA Magazine, 143*(2), 10. Retrieved from ABI/INFORM Global. (Document ID: 1980037281).

Williams, R. (2009). Millennials poised to take over the workplace. *Psychology Today*. Retrieved from http://www.psychologytoday.com/blog/wired-success/200906/millennials-poised-take-over-the-workplace.

Yukl, G. (2002). *Leadership in organizations* (5th ed.). Singapore: Pearson.

[Authors' Note: This research was conducted under the Ka-Bar Leadership Program. The program is sponsored by the Director of Intelligence, Headquarters, U.S. Marine Corps, and is facilitated by Myra Dingman and Susmita Murthy of the Deloitte Consulting LLP.]

Dr. James E. McGinley is a Branch Head at the Marine Corps Intelligence Activity (MCIA) and is an adjunct faculty member at Northcentral University. Tim Weese currently serves as the Operations Officer for the Intelligence Operations Division, Intelligence Department, Headquarters, Marine Corps. Jennifer Thompson is the Special Security Officer at MCIA. Kevin Leahy is an information technology specialist at MCIA.

Pakistan Approaching Zero Hour:
A Fast, Fanatic, and Furious Ritual

by Anita Rai

On every accessible form of media we recently watched a most horrific scene from Pakistan. Malik Mumtaz Hussein Qadri, the bodyguard turned killer of governor of Punjab Salman Taseer, received a shower of rose petals. When the self-confessed murderer was taken to the court, a large raucous crowd gave him an exuberant welcome. The smug killer was hailed and congratulated with hugs, pats, garlands of flowers, and kisses. As cameras flashed, the super-contented killer smiled and shouted *Allah ho Akbar!* Police officials who had Qadri in their custody were thrilled to have a *ghazi*[1] in their midst! Lawyers notably affiliated with PML(N)[2] were conspicuous by size and sprightliness in their support and admiration for Qadri, a cold-blooded murderer. Fazlur Rehman Niazi, President of the PML(N) Islamabad Lawyer's Forum, led them in a zealous celebration of a new-found hero as a fanatic killer. Niazi had the perverse pleasure of garlanding Qadri on behalf of a large number of colleagues whose profession it is to defend the "law" of Pakistan. This raises the question: *What is more damaged? The Law or the State?* By condoning a criminal like Qadri, black-coated legal counsels from among the "moderate" majority in Pakistan demonstrated that despite a Western packaging of coats, pants, and boots, they are fundamentally the same as the fatwa-fathering malevolent clerics who with unrelenting ruthlessness triggered murderous Islamists to pull the trigger on an avowed pluralist, Salman Taseer.

The sheer number of "moderate" Pakistanis who stated unequivocally that Mr. Salman Taseer deserved to die for his "blasphemous" action in trying to get justice for an alleged blasphemer, Asiya Noreen – an impoverished Christian labourer and mother of five – is shockingly real. From podiums and pulpits, prayer gatherings and public meetings, the devious *mullahs*[3] "inspired" fellow faithful to take things into their own hands and show how faithful they are to their faith and Prophet. Taseer was declared a *murtad*[4] and a noisy demand was also made to dismiss him from office. It is understood that Mumtaz Qadri is associated with a Sufi-Muslim group *Daawat-i-Islami* (Islamic Invitation) and not the Taliban, al-Qaeda, or any other confirmed terrorist organisations. *Daawat-i-Islami* is inclined toward Barelvi Islam, a Sunni sect that of old is a strong claimant of moderate Islam. Following Qadri's act of murder, *Ahle Sunnat wal Jamaat Pakistan*, a voluminous religious body mostly comprising Barelvi Muslims, issued the following statement: "Muslims should not attend the funeral service of Salman Taseer or even try to pray for him." For these priests of preposterous prejudice, Mr. Salman Taseer was a *murtad*. His punishment therefore, cannot end with his murder alone – a murder these chauvinists have purposely precipitated.

A bigger part of Pakistani media was in perfect sync with the *mullahs* as they first called for the murder of Asiya and later for the murder of Taseer. It enacted a policy of obscuring those members of the *mullah* mafia who declared lucrative financial rewards for whoever murdered Taseer. There is evidence aplenty; Pakistani Vernacular Media (Urdu) was a party to the evil machinations leading to Taseer's murder. PML(N) leadership and members had always harboured severe antagonism against Taseer. With the *mullah* and the media already having launched a hate campaign against him, the Sharif brothers[5] had no reason to hold back. They threw themselves into a vindictive smear campaign to sully his image in front of the Muslim community of Pakistan. The hate machinery hungering for his head ran endlessly with the government taking no action at all to stop or restrain this macabre affair conducted by mullah, media, and pseudo-intellectuals, who are widely believed to be from the moderate majority. The moment it became clear that, no matter what, Taseer was fully resolved to help Asiya, his PPP[6] colleagues also abandoned him.

As soon as the governor collapsed in a pool of blood, the "Pakistan Mullah League" [phrase coined by the author] and a better part of Pakistani Media rejoiced in the killing of one of the country's most endangered species of sane minds. The number of "moderates" from the rank and file of Pakistani society who zealously came out in support of the governor's assassin makes one's blood run cold. Clerical leadership right across the board of Pakistani Muslims immediately endorsed Taseer's murder. Condemnation by party and opposition politicians was slow and reluctant. Messages of condolence did not take as long. Nevertheless, they were underlined with the view

that his desire to get the bigoted Blasphemy Law amended and his inflexible determination to help an alleged blasphemer get justice in the form of a Presidential pardon could not have ended differently. The Archbishop of Lahore, Lawrence John Saldanha, categorically condemned the murder and the Minority Affairs minister, Shahbaz Bhatti, a Catholic by faith, announced observation of a 2-week mourning period.

Pakistan can no longer screen its socio-political realities with any smoke. Many people are dangerously mistaken to think that this is the first time Islamist fanaticism is at an all-time high in Pakistan.

The only good to come out of this most tragic business is Pakistan can no longer screen its socio-political realities with any smoke. Many people are dangerously mistaken to think that this is the first time Islamist fanaticism is at an all-time high in Pakistan. The truth is, Pakistan had already started to see a surge of Islamist fundamentalism in the twilight years of the life of its founding father, Muhammad Ali Jinnah. One particular Muslim cleric cannot but be credited for this fatal feat. *Maulana*[7] Abul ala Maududi (1903-79), an early 20th century Muslim scholar and political activist, and inspiration for the likes of Sayyid Qutb of Egypt and Ruhollah Khomeini of Iran, was by his own admission a virulent enemy of democracy, pluralism, and gender equality. He would go on to form an Islamist political party whose well-organised propaganda machinery disseminates his theo-political literature all over the world. Millions of Muslims hold Maududi in very high esteem. Maududi insists that if a Muslim proves to be an apostate he or she must be killed. He has written in detail on Islamic law and jurisprudence in his book, *The Islamic Law and Constitution*. Mark Gould from the Hoover Institution says:

> When a non-Muslim reads Maududi's characterization of an Islamic state, where shari'ah will be enforced, and his characterization of why this state will be beneficial and freedom-enhancing for non-Muslims, s/he is likely to be either baffled by Maududi's ability to present second-class citizenship as beneficial, or outraged by his audacity.[8]

Not surprisingly, Maududi enjoyed immense patronage of the Saudi government and clergy, which have bestowed many honours upon him.

A staunch opponent of Pakistan, Maududi did not let many opportunities go by without discrediting and belittling Mr. Jinnah. Endowed with a sharp intellect, Western education, and secular outlook, the well-bred, well-read, well-groomed, and well-cultured Jinnah was too far removed from Maududi and his take on religion and politics.

> Mawdudi opposed secularism because he thought it to be anti-religion, and opposed democracy as it meant the dominance of Hindus in the Indian context. He opposed Pakistan because he believed nationalism, particularly Muslim nationalism, was against Islam. According to his definition of Islam, all those who accepted Islam were one nation and those who did not were a different nation.... Mawdudi was opposed to both the Pakistan movement led by the Muslim League and the freedom movement led by the Congress.... He continued to oppose Pakistan and his opposition became shriller with the approaching possibility of the partition of the country (India).[9]

Muhammad Ali Jinnah strove for a separate state in the form of Pakistan and succeeded. However, he did not want it to be an Islamic state in the same way as contemporary Islamic countries. He knew that Pakistan would be a Muslim-majority country, but one with its non-Muslim minorities as equal stakeholders.

Delhi, 1943: The All India Muslim League session, April 14-26. Muhammad Ali Jinnah, its president, thus spoke to his audience:

> The minorities are entitled to get a definite assurance or to ask: "Where do we stand in the Pakistan that you visualise?" That is an issue of giving a definite and clear assurance to the minorities. We have done it.
>
> We have passed a resolution that the minorities must be protected and safeguarded to the fullest extent, and as I said before, any civilised government will do it and ought to do it...[10]

To the Associated Press of America, Jinnah said:

> Hindu minorities in Pakistan can rest assured that their rights will be protected. No civilised government can be run successfully without giving minorities a complete sense of security and confidence. They must be made to feel that they have a hand in government and to this end must have adequate representation in it. Pakistan will give it. (8 November 1946)

On 21 May 1947, Mr. Jinnah was interviewed by Reuters' star journalist, the late Archibald Doon Campbell, who a

few months later would break the news of Gandhi's assassination to the world.

> Campbell: Do you envisage the formation of a Pan-Islamic state stretching from the Far and Middle East to the Far East after the establishment of Pakistan?
>
> Jinnah: The theory of Pan-Islamism has long ago exploded, but we shall certainly establish friendly relations and cooperate for mutual good and world peace...
>
> Campbell: What are your views in regard to the protection of minorities in Pakistan?
>
> Jinnah: There is only one answer: The minorities must be protected and safeguarded. The minorities in Pakistan will be the citizens of Pakistan and enjoy all the rights, privileges and obligations of citizenship without any distinction of caste creed or sect. They will be treated justly and fairly. The Government will run the administration and control the legislative measures by its Parliament, and the collective conscience of the Parliament itself will be a guarantee that the minorities need not have any apprehension of any injustice being done to them. Over and above that there will be provisions for the protection and safeguard of the minorities which in my opinion must be embodied in the constitution itself. And this will leave no doubt as to the fundamental rights of the citizens, protection of religion and faith of every section, freedom of thought and protection of their cultural and social life.[11]

Like many other Islamist clerics and ideologues, Inayatullah Khan was also against Jinnah and his idea of Pakistan. Popularly known as Allama Mashriqi (1888-1963), he founded the *Khaksar Tahreek* (Humble workers Movement) (1931), a predominantly Muslim paramilitary organisation devoted to restoring the power of the Islamic empire by reviving its former glory. Mashriqi, a Cambridge-educated mathematician, deeply admired Adolf Hitler, whom he met in 1926. The way Mashriqi taught, trained, and ran the *Khaksars* (humble workers) is indicative of the strong influence Hitler had on him. To him the *Khaksars* were the Indian equivalent of the German SS and he led them accordingly. Mashriqi, who vehemently opposed the partition of India, was obsessed with his dream of Muslim rule in India. One can understand his animosity toward Jinnah from the fact that, in 1943, a *Khaksar* made an attempt on Jinnah's life. After partition, Mashriqi migrated to Pakistan and founded a party called the *Islam League*. It failed to emerge as a significant political party but succeeded in grafting Mashriqi's ideas onto the minds of many Muslims—ideas that Jinnah considered crazy and irrational.

The Muslim League, led by Jinnah, was not aiming for an Islamist Pakistan. This led Maududi to say that Pakistan would be *napakistan* (unholy land). Through an article in *Tarjuman-ul-Quran*, Maududi proposed to establish a party of the righteous. Only a handful of Muslims responded. A few months later, he founded *Jamaat-i-Islami* (JI), with himself as its *Amir* (Head). The sole objective of JI was to work toward building an Islamist state. As much as he was opposed to Jinnah's *napakistan*, the inevitability of partition was not lost upon him. Two weeks after Jinnah led Pakistan into freedom, Maududi migrated through a brand new border to Lahore.

> Apprehensive that a secularist "ignorant of even the ABC of Islamic *Shariah*" (Maududi 1960: 43) would abolish the public role of Islam as in Kemalist Turkey... Maududi threw himself into direct competition with the Muslim League for the leadership of the new Muslim state.[12]

Ever since Maududi had founded the Jamaat-i-Islami in 1941, JI had been demanding an Islamic Pakistan. Four months after the creation of Pakistan from within the subcontinent and seven months before the death of its prime architect, Maududi delivered two lectures in the Law College of Lahore. In these lectures (6 January and 19 February 1948), he pressed the Constituent Assembly of Pakistan to codify an Islamic Constitution and provided specific guidelines. He designed the case for Islamisation to arouse the Islamists in Pakistan. Maududi took advantage of the uncertainties baffling the leadership in its efforts to ascertain the right governing framework for the new country and tried his best to convince the people that the only certainty of Pakistan succeeding was as a full-fledged Islamic state. In *The Vanguard of the Islamic Revolution: The Jamaat-i Islami of Pakistan* (University of California Press, 1994, chapter 6), Nasr mentions that Raja Ghazanfar Ali of the Muslim League and Faiz Ahmad Faiz, a renowned literary figure and editor of an English language daily, were among those prominent Pakistanis who were quick to defy this disturbing conviction.

From 23 March 1956 onward, with the enforcement of its first constitution, Pakistan was renamed the "Islamic Republic of Pakistan."

With Jinnah passing away there was no stopping Maududi. Pakistan's political leadership became great pals with

obscurantist Muslim clerics, especially those who prior to partition were against the very idea of Pakistan. The government willingly allowed them to interfere in the formulation of the Constitution and call the shots in finalising the governing model! Jinnah's lieutenants came out from the masks they used to wear when he was there. Their heartfelt wish came true in the shape of the Objectives Resolution. The country's first Prime Minister, Liaquat Ali Khan, presented the Objectives Resolution in the Constituent Assembly on 12 March 1949. The main principles of the Resolution incorporated *Sharia* principles, which would form the base of the Constitution of Pakistan. It promised the Muslims freedom, democracy, equality, and justice "in accord with the teachings and requirements of Islam," encouraging the JI to interpret the resolution as clear expression of the government's intention to make Pakistan a theo-democratic Islamic state. So much for Mr. Jinnah's declaration broadcast to Americans and Australians in February 1948 that no one should make the mistake of thinking that Pakistan is a theocratic state, "to be ruled by priests with a divine mission." Jinnah's Pakistan substantially ended up in the hands of a control freak clergy, never since restored to its original objective. From 23 March 1956 onward, with the enforcement of its first constitution, Pakistan was renamed the "Islamic Republic of Pakistan."

When the 20th century kicked in, Karachi, the largest and most populous city of Pakistan, had more than 2,000 Jews living in it. In 1893, they had built the *Magain Shalome Synagogue* at the junction of Nishtar Road and Jamila Street. Lahore and Peshawar also had Jewish communities but Karachi was more important, which is why in 1918 the All-India Israelite League convened there. In May 1948, *Magain Shalome* was torched and Jews were attacked. With each Arab-Israeli conflict (1948, 1956, and 1967), the anti-Semite hostilities in Pakistan increased. This resulted in migration to India, the UK, and Israel. With a decree from the Islamist dictator General Zia ul-Haq, *Magain Shalome* was torn down to make space for a shopping centre. Today, only a few dozen Jews live in Karachi. The elderly still speak in Urdu and Marathi.[13] In a country with a fast-fanning fan-following of fanatic Islam, these Jews consider it prudent to pass off as members of the *Parsi* community (Zoroastrians).

The fact is, Pakistan's public psyche and discourse are controlled by Islamist intolerance for everything non-Islamist and secular. Far right Islamist views prevail. Islamists who had advocated for Taseer's murder are now actively advocating for the freedom of his murderer. Mr Taseer himself had often observed that dangerous extremist organisations are thriving under the very nose of the Establishment, especially the military and intelligence. The state "superiors" do not look the other way. In an "Islamic Republic," when wars are waged on infidels, they do not have to. In as vastly a Sunni-Muslim majority country as Pakistan, discriminatory policies and legislation help sustain a markedly intolerant society, with a strong penchant for violence in the name of Allah. The Shia Muslims (Twelver, Ismaili, and Bohra) remain the worst hit among Pakistan's minorities. They are a permanent target for disproportionate killings, both mass and individual. Christians, Hindus, Ahmadis, Bahais, and Sikhs share a fate of an understood "policy" of compulsion and marginalisation. The government does not permit Bahais to go for pilgrimage to the *Bahai World Centre* in Israel.

Every sphere of Pakistan is permeated with hard-line Sunni ideology.

Every sphere of Pakistan is permeated with hard-line Sunni ideology. Admission to all government-backed educational institutions requires declaration of religious denominations by applicants. Non-Muslim students must get their affiliation to respective religions certified by the religious head of their local community. State-run schools make it compulsory for Muslim students from all sects to study *Islamiyat* (history and tenets of Islam as presented in the Hanafi school of Sunni Islam). Non-Muslim students do not have the opportunity to study equivalent courses of their respective religions. Most of these schools also make the non-Muslims study *Islamiyat*. It is mandatory for Muslim students to submit in writing the affirmation of their creed: Muhammad is the Seal of Prophets and they believe in his Prophethood. This makes life yet more distressing for the Ahmadis who believe Prophet Muhammad was succeeded by another prophet, Mirza Ghulam Ahmad.[14] Although they consider themselves to be Muslims and practice as such, a Constitutional amendment in 1974 proclaimed that Ahmadis are non-Muslims. In 1984, General Zia ul-Haq made another legislative enforcement of this declaration. Sections 298-B and C were added to the Pakistan Penal Code. Ahmadis are prohibited from identifying themselves as Muslims in any form and manner. Following is an excerpt:

> Any person of the Quadiani group or the Lahori group (who call themselves "*Ahmadis*" or by any other name), who, directly or indirectly, poses himself as Muslim, or calls, or refers to, his faith as Islam, … shall be punished with imprisonment

> of either description for a term which may extend to three years and shall also be liable to fine."

Ambiguity of the phrase "directly or indirectly" is exploited by Muslim clerics to settle personal animosity and/or incur material gain. On numerous occasions, false charges have been brought against the Ahmadis—so much so that they cannot use the standard Islamic greeting *Salam Aleikum* and name their sons Muhammad without earning charges. They do not have access to Muslim cemeteries. While some of their mosques were desecrated, many others have been forced to close down. The government prohibits them from performing *Hajj* (the Muslim pilgrimage to Saudi Arabia). On 10 August 2009, in a village near Faisalabad, Punjab police officials plastered the *kalima-e-shahadat* (words bearing witness to Allah and His Prophet) on the walls of an Ahmadi mosque. Sacred blessings and invocations on doors and exteriors of homes and shops were hammered out. Tiles bearing the names of "Allah" and "Muhammad" were dumped into sewage drains. Similar behaviour by a non-Muslim constitutes blasphemy and he or she will face charges right away.

Minority Rights Group International reports say that Pakistani minorities are suffering increased attacks, repression, and displacement. More and more minorities are leaving Pakistan. The Taliban demand – that non-Muslim minorities in the FATA[15] either convert or pay *jaziya* [the tax Muslim rulers exact from *dhimmis* (non-Muslims ruled by Muslims)], or leave Pakistan – has also forced many to leave their country.

> The Hindu population has declined over the years as they opt to leave the country or become Muslim to avoid discrimination ..."These days we Hindus live in fear and with a constant sense of insecurity," Amarnath Motumal, a Hindu community leader and lawyer, said, adding that one reason for this is the kidnapping of Hindu girls who are then married off to Muslim men and converted to Islam.... 10 to 15 such abductions took place each month in the Lyari locality of Karachi alone. "Many more occur in rural areas of Sindh but not all families want to talk about them," he added.... in Balochistan Hindus are being "picked up" by security forces because they are perceived as backing nationalists in the province who are waging a struggle for autonomy. "These persons are labelled as Indian agents backing nationalists even though they have lived in Balochistan for generations and have no links with India," Mr. Motumal said.... In May 2008 a Hindu factory worker was killed on blasphemy charges while a year later Hindus came under attack in the town of Umerkot following another charge of blasphemy.[16]

Asiya's world has closed in upon her. The longer her imprisonment continues, the flimsier is her chance of ever receiving help from anyone outside the confines of the prison walls. Pakistan right now does not look too favourable for a down and out minority woman who also happens to be an alleged blasphemer. Clerics across deep sectarian divides have warned the government that they have already sealed Asiya's fate with a death sentence. They have not minced their threat: Whoever would commit the heresy of trying to set her free, or even support her, will soon join Salman Taseer. The President of Pakistan refuses to comment on this matter and the Prime Minister promises that the "Blasphemy Law" is untouchable and will stay untouched. These people do not realise that this promise and every promise like this is a betraying breach of the promises made by Muhammad Ali Jinnah to the people of Pakistan. Scores of minority members have suffered in the past. Their condition is going to change but for the worse. So long as the baneful Blasphemy Law introduced by General Zia stays put and the values that sustain such filth reign supreme, no Asiya is safe in Pakistan. With Pakistan approaching zero hour fast, fanatic, and furious, no one willing to stand up for any Asiya is safe, not even a Muslim.

Anita Rai is the author of the recent volume Jihad and Terrorism. *She holds a BA with Honours in English Literature and Language, with History and Political Science as supplementary subjects, from Calcutta University in India. She also has an MBA with a specialization in Marketing from the University of Lincoln in the UK.* Jihad and Terrorism *was preceded by other books on her personal journey, the history of Islam, and comparative religion. The latest work's unique contribution has been endorsed by the best minds in the field. Following 9/11, Rai has been deep-searching the history of Islam and Islamism. As a result,* Jihad and Terrorism *provides some much-needed and long-awaited answers to pertinent questions regarding today's plague, terrorism. Rai is a contributing writer for the Research Institute for European and American Studies (RIEAS) and the* Islam, Islamism, and Politics in Eurasia Report (IIPER). *Currently, she is working on a project on Iranian Islamism/Khomeinism. Her insider insight is based on years of extensive research in seeing the revelation of vital facts. Anita lives with her husband in London.*

Notes

[1] A veteran Muslim warrior.
[2] Pakistan Muslim League (Nawaz).
[3] Muslim clerics.
[4] Apostate.

[5] Nawaz Sharif and Shabaz Sharif, top leadership of the PML(N).
[6] Pakistan People's Party.
[7] A common title used by a Muslim cleric.
[8] *Understanding Jihad: An Authentic Islamic Tradition*, The Hoover Institution Policy Review (February & March 2005), No. 129.
[9] Kalim Bahadur, "Islamic Parties in Pakistan," in John Wilson, ed., *Pakistan: The Struggle Within* (Dorling Kindersley (India) Pvt Ltd., 2009).
[10] *The All-India Muslim League, Delhi session, April 1943: Verbatim report of the presidential address*, printed by S. Shamsul Hasan (Muslim League Printing Press, 1945).
[11] *Deccan Times*, India, 25 May 1947.
[12] Elora Shehabuddin, *Reshaping the holy: democracy, development, and Muslim women in Bangladesh* (USA: Columbia University Press, 2008), chapter 4.
[13] Official language of the state of Maharashtra, India, mostly spoken by Marathis/Maharashtrians.
[14] Mirza G. Ahmad founded the Ahmadi sect at a place called Qadian, North-West India, in the 19th century.
[15] Federally Administered Tribal Areas.
[16] Shafqat Ali, "Fear Forces Hindus to Leave Pak, or Convert," *The Asian Age*, 10 January 2011.

An Afghan Democracy

by Garett B. Tippen

INTRODUCTION

In Afghanistan, the ISAF (International Security Assistance Force) is currently at a cross-roads not only due to the security situation but more importantly, I believe, because of the political future of the country. The outside, and especially Western, world clamors about the corruption that it sees choking the country's ability to grow and modernize. The importance of disrupting corruption is typically a Western concept; we should stop trying to look at Afghanistan and its problems through our Westernized eyes. ISAF must first help Afghanistan establish security and train its security forces to the point where they can control their own internal security situation.

One of the most important factors in establishing lasting security is a coherent legal system to gain the support and trust of the people...

One of the most important factors in establishing lasting security is a coherent legal system to gain the support and trust of the people through simplifying the current legal procedures and making it less complex and more accessible to the average Afghan. Parallel to security, I see the political situation, at this time, as too large and complex for the average Afghan to comprehend. By "simplifying" the political process, ISAF can allow Afghanistan to grow into its own form of democracy, which will most certainly not mirror our own but may be enough to stabilize a country desperately seeking stability and continuity. In this article, I will discuss some of ISAF's honest but naive mistakes, as well as some possibilities that will allow Afghanistan to succeed as an independent and politically stable nation.

COUNTERINSURGENCY (COIN) IN AFGHANISTAN

COIN (Counterinsurgency) is the strategy used by forces aligned with a recognized government, against an insurgency, within its internationally recognized territory.[1] The main point of COIN is to separate the people from the insurgency by delegitimizing the insurgency and establishing the government's ability to provide an acceptable security situation for the general population. In Afghanistan, especially in the southern provinces, the people are the insurgency or the "Taliban." The Taliban should be thought of as a regional militia with regional influence and goals. They are loosely organized and lack any political organization or structure compared to their prior rule in the 1990s. They are more rural-based, from which their influence and their recruiting base derive, but have been recently trying to push their influence into the larger urban areas of Afghanistan. Following the basic concepts of insurgency, the Taliban understand that in order to control the country that they must also control the centers of commerce, education, and politics, i.e., the big cities. The Taliban are also more "regional" as they are more prevalent in the rural southern provinces and more accepted by local rural communities. Whereas in the north, if a young man wants to prove his manhood he might join the Afghan National Army, which is highly respected in many areas of the country, in the south that same young man would join the ranks of the Taliban. The Taliban are not the same as Al Qaeda, which is both a terrorist and a political movement seeking a world Islamic Caliphate. The Taliban is a local and regional institution (to include Pakistan as well) that is an extension of the Mujahedeen fighters which opposed the Soviet Army and its communist puppet state. It came out of the power vacuum created by the Soviet withdrawal and subsequent absence of any political and security infrastructure.[2] The current dilemma is whether to include the Taliban in the political process to make its members more mainstream and less hostile to the national government. The answer is both "yes" and "no."

ISAF must not make the same mistakes that U.S. and Coalition forces made in Iraq with the de-Ba'athification program that forced many average Iraqis out of the political system and alienated a significant portion of the population.

There are two types of Taliban that exist in Afghanistan today: (1) the Old Guard made up the ranks of the Mujahedeen who opposed Soviet occupation and now hold the roles of village elders and tribal leaders, and (2) the new Taliban educated in Mosques and *Madrassas* in Pakistan, who are more fanatical and more willing to target civilians and non-military institutions. There does exist a schism between these two groups as the old Taliban are seeing their traditional leadership roles being usurped or threatened by this new breed of insurgents. ISAF can exploit this division by appealing to the older and more traditional group, whose positions of influence the younger Taliban are threatening. ISAF can show the older Taliban contingency that by supporting the national and provincial government it will be protecting the traditional roles and values of their regions. The old Taliban are now the village elders and traditional leaders of Afghanistan and should be brought into the current political process. They will hold more influence among their villages and tribal areas than the currently more fanatical and violent breed of Taliban. As for the new Taliban, those that refuse to lay down their weapons and participate peacefully in the political process must be separated from the rest of the population and delegitimized by the old Taliban and the political process. ISAF must not make the same mistakes that U.S. and Coalition forces made in Iraq with the de-Ba'athification program that forced many average Iraqis out of the political system and alienated a significant portion of the population. As in Nazi Germany of the past, if an Iraqi wants to hold a government position or even teach in a government-run school, he or she has to be a member of the Ba'ath party. ISAF must accept that the Taliban exists as an important and excepted element of Afghan society, especially in the southern regions, and that it would be a dangerous mistake to not incorporate its members into the current political system.

The goal that ISAF should be striving for in Afghanistan is to establish a relatively stable country where terrorist networks such as Al Qaeda cannot operate, plan, and train—undisturbed—for attacks against the West. Now, I did not mention a "relatively stable democracy," as I believe that it may not be in ISAF's best interest to force our Western concept of government on the Afghan people without incorporating into it the realities of the Afghan culture and their own tribal variations. ISAF should not abandon the parliamentary system currently in place, merely adapt it to the cultural realities on the ground. NATO and ISAF forces need to understand that there must be two different adaptable political systems as well, one for the large city hubs and one that is tailored for the areas outside the influence of these urban centers. ISAF must cast aside the Western concepts of "good and evil," "right and wrong," and understand that our current political strategy will not necessarily work in Afghanistan, that is, our insistence on a parliamentary democracy and not seeking a more realistic political situation (pushing power down to the provincial and district levels), tribal and linguistic differences, and the poor showing of the majority of ISAF forces in theater that lack adequate U.S. forces to make up for ISAF weaknesses. This will be discussed in the following pages.

General Petraeus is correct in trying to adapt the COIN and surge strategy that worked in Iraq and turn it into a plan that will also succeed in Afghanistan by securing the larger cities first, for example, much in the same way the surge established security and support for the security forces in Iraq, and especially in Baghdad. However, an entirely different approach has to be taken with the "rural" areas of Afghanistan. ISAF should follow two entirely different strategies, with both plans working, side by side, with differing short-term goals but with an ultimate final goal of a stable and secure Afghanistan. The COIN strategy that worked in Iraq can be applied and work to secure the major cities of Afghanistan, but a different "grass roots" approach must be taken with the areas that lay outside the influence of the larger population centers. This is nothing that is new or overly dramatic in this type of strategy as any counterinsurgency practitioner can attest. Most insurgencies will have two differing strategies for rural and urban situations. Hence, to be effective, the government and security forces must also have two different plans for dealing with the insurgency in both urban and rural settings.

An Afghan National Army security checkpoint in Kandahar Province, date unknown.

The large cities of Afghanistan must be considered different "areas of operations" from the rural regions of the country. Kabul and cities like it are alien to the average rural Afghani to the point they are considered a separate group, such as is the case for the inhabitants of Kabul who

are referred to as "Kabulies." Comparing the big cities to rural Afghanistan is like night and day. The city of Kandahar has a very different culture that includes social and political factors which differ from those in the Province of Kandahar. The urban Afghan is more likely to be concerned with and involved in the political system than his rural counterpart. He is more likely to see the tangible effects first of the positive or negative impact of the political system than someone out in the hinterlands. He will also be more apt to support the government and its security forces if he can see positive results. As seen in Baghdad, traditional COIN strategies can be effective in the large urban centers of Afghanistan by creating security checkpoints, constant patrolling, meeting minimum government obligations of public works, and creating and supporting social and government programs. These simple steps will work to secure the cities against the influence of the insurgents. These are the steps that ISAF, under General Petraeus, has been taking as current and future operations look to secure the large urban areas against the Taliban.

Rural Afghanistan must be handled cautiously in comparison to the county's urban centers.

Rural Afghanistan must be handled cautiously in comparison to the county's urban centers. ISAF should not force democracy on the goat herder who is only concerned with his own immediate center of influence, his family, his goats, and his security. The current push to bring the villages and towns of rural Afghanistan into the political process is to encourage them to elect *Maliks*, an Arabic word for "chieftain." The term Malik is prevalent among the Pashtun cultures for identifying their tribal leader—an individual who basically acts as a village mayor and can represent the community.[3] Traditionally, Maliks were not chosen through individual election. In the present political system, to encourage the population to take part in the political process, ISAF is requiring that villages elect a Malik If they want to receive aid from the government or ISAF. In order to participate in the political process, villages and communities must first be represented by "elected" Maliks who can represent their interests at district and provincial *jirgas*. The only problem is that this undermines the current system of power which exists in rural Afghanistan in which village elders and religious leaders hold influence over their people. By forcing the villages to democratically elect their Malik, ISAF is undermining the very authoritarian structure that we want to cultivate and ultimately to have support the political process. Again, ISAF must adapt the democracy to the realities on the ground. While in the larger cities traditional elections for political appointments can work, in the rural areas democracy must be adapted to the situation. Until the whole of Afghanistan is ready and able to comprehend the dynamics and complexities of a parliamentary democracy, we need to work with the traditional system that is currently in place. ISAF must not alienate those individuals who hold traditional roles of power and influence or we will force them to side with an insurgency that shares many of same traditional values and roles. ISAF needs to allow Afghanistan to "grow" into democracy, and it should be acceptable to have one part of the country, the large urban areas, to outgrow their rural brothers. As democracy and its positive aspects develop in the larger cities, the village and communities of rural Afghanistan will then have a light to guide them forward.

MISCONCEPTIONS

The first mistake that the U.S. made when deciding the fate of a future Afghanistan was to ignore the overtures of the former King of Afghanistan, Mohammed Zahir Shah, who had offered to return to his former country, not as its king, but as a unifying symbol. The U.S. was opposed to the return to power of the former monarchy as it would be a deterrent to the representative democracy Americans hoped Afghanistan would adopt. The former king went even further to alleviate these fears, insisting that he would not even seek any ministerial roles in the government but only act as a symbol for the Afghan people. The first Afghanistan *Loya Jirga* in 2002, made up of a diverse group of former warlords, returned exiles, and military figures, enthusiastically endorsed the return of the former king and voted overwhelmingly to welcome him back into the country. Due to pressure from the U.S., through its envoy and State Department officials, this action was blocked and the former king did not return to represent the people.[4] King Zahir Shar died in 2007; only his son remains to represent the royal line, but he has never lived in the country.

The U.S. let an opportunity for internal cohesion slip through its hands by not supporting the return of a symbolic unifying figure to the country that sorely lacked any unifying elements. In a region with diverse languages, tribal affiliations, and familial ties that serve only to splinter the country, King Zahir Shah could have acted as a simple symbol for a people desperately looking for stability and continuity – a symbol that could have hosted *Jirgas*, settled tribal and territorial disputes, and acted as a liaison with neighboring countries until a permanent and settled parliament took office. The king could even have moderated disputes and settled claims within the new parliament itself. A locally recognized "father of the country," the king would have been a figurehead for the

average Afghani civilian to look up to and to represent the entirety of a severely diverse and broken nation. The U.S., in its naivete, saw the spreading of democracy as its final objective, and the appearance of the former monarchy was too alien a view to consider for even a short-term solution.

The second mistake by the US was to allow ISAF, a construct of NATO, to take over the security of the country. While the U.S. may have not have had a choice due to its limitation in resources and manpower, split between Iraq and its already standing obligations, it made an error in assuming that NATO nations could fill the security void. In turning security operations over to coalition forces in 2005, the U.S. unleashed on Afghanistan an inexperienced and passive army. The problems are familiar now and legendary within the U.S. military, if not known by the general public, and borne out of political liability and the hope to present a unified front against the insurgency. Therefore, a face of cooperation was presented. The stories are legendary of ISAF forces refusing to leave the wire; or not going beyond the effective range of artillery, refusing to engage the enemy or, even worse, paying off local insurgent commanders to not engage their convoys as they conducted operations; refusing to conduct security operations on weekends or fly even routine missions after nightfall. And for those few nations that proved ready to fight, they then lacked the resources to effectively bring the fight to the enemy without assistance from U.S. forces. The few militaries that had a fighting capability lacked the ability to effectively move frequently in and around the battlefield without the assistance of U.S. military transport and convoy support. What Afghanistan has shown is that, for far too long, NATO has too heavily relied on the U.S. to act as its military arm. While the end of the Cold War may have signaled the end of large standing armies, Europe saw it as essentially its termination of NATO military obligation. These nations fell back on their main weapon of old, the art of diplomacy, which had failed them miserably in the past and would not prepare them for the "wars of the future." Many of the nations that sent military forces to Afghanistan did so with restrictions that would reduce the possibility of casualties and most certainly reduce their effectiveness in the theater of operations. Once again, European and NATO forces believed they could rely on the U.S. to fight the good fight or, even worse, believed they only had to fulfill a minimum obligation. In a battleground that was closer to their backyard than our own, Europe, again, showed its aversion to the use of force for whatever reason. NATO must be realistic in dealing with future operations in that there are only a few nations whose armies have the ability to deploy and fight effectively (e.g., the U.S., Canadian, Australian, and British armies routinely train and plan together and have shown they can work effectively together as a deployable and militarily effective arm).

The average Afghan citizen, urban and rural, wants security and stability above all else.

With all the above-mentioned problems, the security situation took a downward spiral and the vacuum created by the lack of effective ISAF and Afghan security force operational presence allowed the Taliban to once again step in. It must be noted that there were only three periods of relative stability and security, with the last being under Taliban rule during the 1990s. For all the despicable acts of inhumanity conducted by the Taliban regime, especially against women in terms of both their social and educational roles, it still has to be said that the Taliban was able to bring stability and security to a nation torn apart by political, religious, and tribal upheaval.[5] First and foremost, the average Afghan citizen, urban and rural, wants security and stability above all else. Even though many Afghans did not support the extremes to which the Taliban went, they still appreciated the relative stability the regime brought to the country. With the handover of Afghan security in 2005 to ISAF forces, a security vacuum developed where once U.S. forces patrolled or convoyed. The majority of ISAF forces were content to remain on their bases or just do the minimal amount of life-sustaining convoy operations. The Taliban, just like in the early 1990s following the collapse of what remained of the Soviet-backed government, stepped in to fill the security vacuum. The sentiment was that "a bad cop was better than no cop at all." He may take your money but he probably will not kill you afterward. The current ANP (Afghan National Police) has also failed in this role and until its members can be trained up to adequately take over the security role, the ANA (Afghan National Army) should be given more influence and reach into the provincial and district levels. This will be discussed more under "Judiciary and Policing."

DEMOCRACY IN AFGHANISTAN

A parliamentary democracy is only second in complexity to a representative democracy. Like a representative democracy, a parliamentary democracy requires an educated constituency to understand the system and the patience to understand that system and that its institutions will take time to work. It also requires the majority of the population to recognize a political center of power and to accept and adhere to the political

rulings that come from this center, both at the provincial or state level and the national level. Afghanistan lacks all these essential elements; its weak educational system and an extremely high illiteracy rate do not allow its citizens to understand and comprehend or appreciate the complexities of a parliamentary democracy. Because of the chasm that exists between the general population and the current political regime in terms of basic educational requirements and individual understanding of the system, there is a danger that the Afghan people will become more and more disenchanted with the political process and in turn become antagonistic toward the process as a whole. Without active participation by the populace, understanding the issues and then voting, a democracy can become a malaise of political groups that only use the people to further their own minority issues. An example is present-day Thailand, where the elite whip up the population into a frenzy and personal interests overtake popular consent. Without the support and the trust of the people, representative and parliamentary democracies will fail miserably. Without an educated and understanding population, a democracy will become nothing more than organized chaos.

It has been asked why, as in Iraq, NATO/ISAF has pushed for a parliamentary form of democracy in Afghanistan and not a representative democracy such as we have in the U.S. The answer, as discussed in the above paragraph, is one of complexity. In a representative democracy, the people vote for individual candidates, from the president down to the local county sheriff. In a parliamentary democracy the people vote for the party and not for the individual (although a particularly charismatic person may arise in a party). The party that wins the most votes still has to work with the other parties (usually the ones that also had strong showings) to form a working government. It is through cooperation and negotiation that the winning party is able to seat a government, appoint political positions, and manage national resources and economies. In an especially fractious environment, this forces the political parties to work together and does not allow any one party, or especially any one individual, to gain too much power and control.[6] That is the ideal, of course, but we can see what happens when religion and personal interests come into play, such as in Iraq. While many people are seeing the current political turmoil in Iraq as a failure, I think they are missing the point. Yes, there is political chaos that is trickling down and affecting the current security situation, but that is the beauty of a parliamentary democracy. It is forcing the politicians in Baghdad to work together and form political coalitions, creating backroom deals but, at the same time, not letting any one person take too much power. The Iraqis have two choices: (1) work together, form partnerships, and cooperate politically, or (2) return to the dark days of 2005-2007. While the politicians may be arguing, throwing shoes, and back-stabbing each other, at least they are still only talking about, and not forming, personal militias.

ISAF must cultivate interest in the political system at the local level even if it means allowing latitude in the way the Afghans choose their representatives.

One aspect of a parliamentary democracy that should be eliminated is the ability of the ruling party, coalition, or the Prime Minister to appoint provincial and district governors and city mayors. The political process that affects individual provinces should be pushed down to as local a level as possible. Provinces should be treated and given the basic governing rights that we afford our own states in the U.S.[7] They should be allowed to appoint their own political leaders based on provincial and localized elections, and political appointments should be decided by the winners of these local elections, who will have to form coalitions to form effective power-sharing governments, and not by the Afghan Prime Minister and his ruling coalition. Governors, mayors, and provincial and district political appointees should be selected by the people who are most affected by the consequences of these roles. Districts should be given the same rights as states and counties in the U.S. and the UK. This will not only encourage the average Afghan to be more involved in the political process by making it local, but will educate him or her more about the overall political process. The provinces will have their own laws and regulations that will be in concert with the Afghan constitution and enforced by the state and national judiciary and government. The provincial and district political process is a microcosm of the national political process and can be used as a learning tool for the Afghan people. ISAF must accept that the rural Afghans may use traditional tribal methods to choose their leaders based on the experiences they value in their leaders—gender, as they will only choose a male; age, which is equivalent to wisdom; knowledge of Islam; and even Mujahedeen involvement, as military prowess is held in high regard by most Afghans (as it is in our own country). The leader who may show up to represent a village or even a district may have been chosen by a group of elder peers and not by a one person/one vote system, and he will be deemed acceptable by most of the Afghans whom he represents. ISAF must cultivate interest in the political system at the local level even if it means allowing latitude in the way the Afghans choose their representatives. As coined by the father of the late Thomas P. (Tip) O'Neill, Jr., former U.S. Speaker of

the House, "All politics are local," and ISAF should make the political process as localized and coherent as possible.[8]

Democracy can work in Afghanistan but it must be an "Afghan Democracy," taking into account that Afghanistan and its people hold different values and traditions.

The brilliance of a democratic system is that it is adaptable to any type of cultural environment just as long we realize the limitations of the system. Democracy can work in Afghanistan but it must be an "Afghan Democracy," taking into account that Afghanistan and its people hold different values and traditions. Geographic environment, cultural and social make-up, educational level, and religion must all be taken into consideration. This may not be politically correct to reduce to writing, but the democratic system must be made to fit the situation. For Afghanistan, ISAF will need to strip away the complexities that require a high level of individual education and understanding until the country improves its educational and political systems and can accommodate a full-fledged parliamentary democracy. ISAF will have to accept the very different ways the indigenous people may choose their political leaders, especially in the rural areas. ISAF must not insist on Western ideals. It must realize the significance of corruption, where security is more important, which only hampers the rebuilding process and instills the idea in the average Afghan that we are trying to impose a foreign ideology. As just one example, trying to build a girls' school in a village that does not want one is not prudent. You have not only endangered the lives of the girls who might attend the school but have effectively emasculated the village elder hierarchy and pushed it out of the decision-making process. If we want democracy to work in Afghanistan, then we must help the Afghanis take "baby steps" and allow them to lead themselves forward. ISAF must build up the institutions that will strengthen and promote a future democracy, such as the educational system, a strong military, and a responsible and proactive police force. Afghanistan must be allowed to "grow" into the democratic political process.

JUDICIARY AND POLICING

An area of weakness of our own making, and one that the Taliban has exploited, is the current judicial system. Corrupt, slow to respond, and totally unfamiliar, the current judicial system only serves to enforce the belief that the government and the legal system are out of reach for the average Afghani. In order to resolve a legal issue, citizens first must travel to the provincial capital, usually pay some sort of fee just to walk through a morass of paperwork, wait several weeks if not months to even get their issue on the docket, and perhaps even have to walk through the same hoops repeatedly. They see a system that is slow, inappropriately corrupt, plagued with unfamiliar terminology and concepts, and seemingly never able to provide solutions, even if the problem is capable of being resolved. That is just one of the main problems with the current government and legal system; the concept is incomprehensible to the average Afghan citizen. If a legal issue is resolved, often it does little to bring about a solution and the claimants are usually left with the same problem, but with less of their own money. Just like the security vacuum, the Taliban have jumped in to fill a unique niche.

Especially prevalent in the south, the Taliban have created a traveling court system where they move from village to village and can act as intermediaries, or judge, jury, and executioner all at once. These traveling judiciaries are usually comprised of Afghan elders, and they apply a combination of Sharia and tribal laws to their rulings. They can apply the harshest of penalties for severe crimes to include banishment and even death. While outsiders might see this as barbaric, many Afghanis see this as expedient. There is no paperwork to fill out, no public employees to bribe, and no lengthy waiting for a decision that may or may not come or even satisfy the original complaint. Yes, some of the decisions handed down by the Taliban court system can be harsh but, again, it is a system that is neither outlandish nor corrupt in the average Afghani's eyes. Many Afghanis see the current government judicial system as what is in conflict with their traditional values and Islamic laws. The one argument that is arising with these mobile court systems is that they can be inconsistent with the traditional role of the village and tribal elder as the overall intermediary for local problems. Also, many of the decisions handed down are indeed heavy-handed and are judged too harsh by those involved. ISAF must understand that this is a possible fracture in an otherwise brilliant Taliban strategy that can be exploited.

The judicial process needs to be pushed down to the district level to make sure there will be compliance by the populace.

The judicial process needs to be pushed down to the district level to make sure there will be compliance by the populace. ISAF must encourage the present government to copy the Taliban's efforts by creating mobile court systems that can easily move within the district from village to

village. These mobile courts would be based out of the current District Centers (DC), as that would afford them a base of operations and static security. At this time, DCs are usually the HQs for the District Police and there is a recent push to emplace a battalion-sized element of ANA (Afghan National Army) in each one as well. While on the move, the members would receive protection from ANA forces and not ANP (Afghan National Police) forces. These mobile court systems should not only be comprised of an educated and vetted judiciary but of vetted and locally respected religious figures as well from the local Madrassas or influential Mosques. These mobile courts would respond to any complaint above the traditional village level and would take into consideration and respect the concerns or relevant points made by local elders and religious leaders. The rulings need to be based on current laws in place, to include traditional local laws and values, and Sharia laws. We must respect the use of Shraria law as it has a history in Afghanistan and is understood and accepted by most Afghanis. By using a legal system comprising of Sharia, tribal, and more modern constitutional laws, the current government can show it still values the traditional systems and values of Afghanistan and also can instruct the people of Afghanistan on the value-added system of a constitutional democracy.[9]

ISAF must respect the traditions and the values of the local population by taking into account the traditional Muslim values as part of a new cooperative legal system. Any issues below the village level or which do not constitute capital crimes should be allowed to be resolved at that village level and then recorded and reinforced by these mobile court systems. ISAF must simplify the current court system and adapt to the situation on the ground; that means beating the Taliban at their own game by meeting or exceeding their ability to quickly respond to legal situations swiftly and fairly. By using the ANA and not the ANP as security details, ISAF will lessen the possibility of local influence and corruption as well as localized insurgent attacks. Also, by using the ANA, it will show the local population that we are not favoring any group or tribal affiliation over another, as local ANP are generally assigned to the same areas from which they come and are often influenced by the their tribal and familial ties.

The failures of the ANP are well documented; ANP influence over the mobile court systems should be as limited as possible. That is why ISAF should strengthen the Military Police branch of the ANA and increased its size to the point where it can act as a national state police but still remain under the control of the ANA. The ANA currently garners more respect than the ANP, and until the ANP can be trained to meet required standards the ANA should be given more of a security role in the provinces and districts. The majority of those who join the ANP do so for the money, and it is said in south Afghanistan that if they were brave men, they would have joined the Taliban. There is also a move by many ANP commanders to bring ANP personnel recruited from other parts of the country into the south to limit local influence and corruption. While this is a positive step, it is only a short-term fix as many of the locals will see these police personnel as outsiders. Until the ANP can prove that it can handle local security situations without being influenced by local power players and corruption, the ANA should take the lead role in both national and local security.

CONCLUSION

ISAF must not make the same mistake that the Soviets and their puppet government did in forcing a Soviet style of socialism on a people ruled by village, tribal, and familial ties. The Soviets thought that by creating a utopian agrarian state, breaking up control of the large landowners, and parceling out the land to the people they would get the backing of the average Afghan citizen. They misunderstood the culture of the people, the ties that bind between family, village, and tribal members, and tried to change a way of life that had existed for a millennium overnight.[10] They also did not take into account the independence of the people and their stance against a system which centralized power and allowed them little say in the politics that would rule their lives.[11] ISAF can also learn from the mistakes made by the Taliban during their time as rulers of the country. While most, at first, welcomed the security and stability brought by the Taliban regime, they soon began to chafe at the Taliban's stringent interpretation of Sharia law and their almost fascist-like attempt to control every element of their daily lives. ISAF can avoid these same mistakes if it allows the Afghan people to lead themselves down the path toward modern democracy that mirrors their own traditions and values. ISAF can do this by drastically simplifying the concept of the democracy it wants to instill and allow the Afghans to incorporate their values and their beliefs into the political process. The beauty of democracy is that it allows the human spirit to remain independent while instilling the importance and growth of the overall community. We do not have to force democracy and a constitution on Afghanistan; we just have to show them the basic principles of the system, support their security situation, and protect them from outside influences that fear the establishment of a stable democracy, albeit an Afghan democracy, in the region.

Author's Note: This paper reflects the author's personal judgments and does not represent the views of any department or agency of the U.S. Government or any other government.

Notes

[1]*Oxford English Dictionary*, second edition, 1989, "insurgent B.n. One who rises in revolt against constituted authority; a rebel who is not recognized as a belligerent."
[2]Matinuddin, Kamal, *The Taliban Phenomenon, Afghanistan 1994–1997*, Oxford University Press (1999), pp. 25–26.
[3]*A Glossary of the Tribes & Castes of Punjab*, edited by H.A. Rose, pp. 413-416, Low Price Publications.
[4]Dorronsoro, Gilles. "The Return to Political Fragmentation." *Afghanistan: Revolution Unending, 1979-2002*. C. Hurst & Co., p. 330.
[5]Dupree Hatch, Nancy. "Afghan Women under the Taliban," in Maley, William. *Fundamentalism Reborn? Afghanistan and the Taliban*. London: Hurst and Company, 2001, pp. 145–166.
[6]T. St. John N. Bates (1986), "Parliament, Policy and Delegated Power," *Statute Law Review* (Oxford: Oxford University Press), http://slr.oxfordjournals.org/cgi/reprint/7/2/114.pdf.
[7]Forrest McDonald. *States' Rights and the Union: Imperium in Imperio, 1776-1876* (2002).
[8]O'Neill, Thomas P., with William Novak (1987). *Man of the House: The Life and Political Memoirs of Speaker Tip O'Neill*.
[9]"Pakistan: Sharia law endorsed in deal with tribal leaders," *adnkronos Inernational* (GMC Group), 2010, http://www.adnkronos.com/AKI/English/Security/?id=3.0.3020547082.
[10]"The Afghans - Their History and Culture," Center for Applied Linguistics (CAL), June 30, 2002. http://www.cal.org/co/afghan/ahist.html. Retrieved September 25, 2010.
[11]G.V. Brandolini. *Afghanistan cultural heritage*. Orizzonte terra, *Bergamo* 64, p. 2007.

The author, Garett Tippin, at the Kabul Army Base firing range, qualifying on a Serbian Zastava M90 Assault Rifle, February 11, 2011.

Garett Tippin is a former U.S. Army Field Artillery Officer who served as ALOC (Administrative and Logistical Operations Center) and Support Platoon Leader during the initial invasion of Iraq and subsequent security operations. He graduated from the University of Missouri with a BA in Anthropolog, and attended the Human Terrain System Course conducted by the Army at Ft Leavenworth, KS. He is also a graduate of OCS at Ft Benning, GA, and the Field Artillery Officer Basic Course at Ft Still, OK. He was an operations and logistics specialist in Al Anbar Province, Al Assad, and Al Qa'im, Iraq, in 2005, a project lead analyst for TF-134 TIFRC (Theater Internment Reconciliation Center) Detainee Operations at Camp Cropper and Camp Taji, Iraq, in 2009, and a senior intelligence analyst for TF Kandahar in Afghanistan in 2010. He is currently a senior atmospherics reports analyst at Bagram Airbase, Parwan Province, Afghanistan.

Please submit any comments or suggestions for improvement to afghanarticles@yahoo.com.

Charlemagne's Tactic:
Using Theology as a Weapon in the Fight Against Al-Qa'ida

by Dr. J.A. Sheppard

Extremism in the Muslim world is not a new topic.

Extremism in the Muslim world is not a new topic. The truth is that there is a substantial body of literature dedicated to finding the root causes that explain the conditions which permit radical movements to flourish. The upshot of these analyses is usually an assessment that provides a range of social causes for the existence of drastic behavior. For example, Dr. Stephen Pelletiere viewed radical Muslim groups as a response to failed secular states.[1] So too, Kevin Siqueira argued that disparate dissident movements will unite for a common political purpose but that competition for resources among those groups causes an escalation in their activities.[2] In a slightly different vein, Hamied Ansari attempted to confirm the hypothesis that religious extremism is a consequence of the breakdown of "traditional solidarities" and "communal ties under the impact of urbanization."[3]

Such explanations are informative. Nevertheless, they suffer from two weaknesses: First, by assuming that there must be a different issue beneath the surface of the radical religious behavior, concerns about social problems, *i.e.*, corruption or poverty, can be illegitimately transferred to an enemy fighter who may not have an actual share in that problem. When this happens, important differences become blurred in ways that muddle the strategy for neutralizing an extremist group. Christopher Fettweis' basic typology of terrorism helps to bring this point into specific relief. As he explained, terrorists groups can be placed into one of two broad categories: "nationalists that kill on behalf of their nation or ethnicity and ideological groups, or those that are motivated by ideas, broadly defined."[4] These two typologies demand different responses and, although countermeasures such as the active promotion of democracy may help to quell the nationalist, such a measure is likely to be irrelevant to an ideologically driven group like al-Qa'ida. The second problem with confusing social or political problems with religious ideology is that it can cause one to overlook the role that doctrines play as a weapon. Indeed, history favors the thesis that doctrinal warfare is moderately effective for reducing the impact of an ideologically motivated warrior.

There is no better illustration of this battle tactic than its use by Charlemagne. He lived well before the invention of the social sciences and, because those methods were unavailable to him, his tactical approach to religion garnered dramatic results. Indeed, Charlemagne viewed religion as an all-encompassing object rather than a condition such as having power, strength, or resistance. One consequence of this view was that he was able to target the focal point within a religion where all of an enemy's resources come together to form a unified effort. Translated into modern terms, he was able to find his enemy's "center of gravity."

With that in mind, the overarching question to be explored is whether or not Charlemagne's method can be applied to a modern aggressor like al-Qa'ida. Finding an answer, however, requires a somewhat mechanical view of religion. Put another way, in basic science the center of gravity is the point at which all of the weight of an object appears to be concentrated. If religion is an object, therefore, attempting to strike at the center of gravity means first having to locate the point in the body where the gravitational force acts. This is perhaps different from military assessments that attempt to view a center of gravity as a source of strength, a critical capability, or a person.[5] Indeed, when religion is treated like an object, the point in the body where gravity acts is likely to be a doctrine that holds the religion in perfect balance. As will be discussed below, in Charlemagne's battle with the Saxons the religious center of gravity was a doctrine of heresy. The same may be true for al-Qa'ida but the diffuse nature of both its networks and its associated movements, combined with its close affinity to Islam, makes the strategic targeting of any doctrine a subtle project.

DIFFERENCE BETWEEN DOCTRINE AND IDEOLOGY

Since the center of gravity for an ideologically motivated warrior probably boils down to a doctrine, it makes sense to begin by clarifying a few terms. On

the surface, "doctrine" and "ideology" may appear to be synonymous. The truth is, however, that the two terms signify very different concepts. The roots of the words help to lay bare this fact. "Doctrine" is derived directly from the Latin term *doctrina* which denotes teaching or instruction. With that in mind it should not be at all surprising that the modern use of the term "doctrine" is commonly associated with articles of faith. Indeed, it is often tied to principles or tenets that are customarily associated with a church or sect. By contrast, "ideology" is a modern word that was coined by the French philosopher Destutt de Tracy and refers to the science of ideas.[6] Translated from the French word *idéologie*, the term now commonly pertains to a political or social philosophy of a nation. More precisely, it properly refers to a systematic body of concepts and often involves the integration of theories that constitute a sociopolitical program. Under this banner, Marxism, Communism, and Democracy are all types of ideology. As Desai Meghnad would have it, "Global Islamism" is also an ideology and this assessment is certainly reasonable to the extent that it is a plan for how to live that is distinct from, albeit akin to, Islam.[7]

The Sunni and Shi'a traditions are of the same ideology, which is Muslim, but they are marked by profound doctrinal differences.

Although the difference between "doctrine" and "ideology" appears to be a distinction between religious and political vocabulary, there is no semantic feature that limits the two terms to the domains of those disciplines. There is, however, a limited logical relationship between the concepts. That is to say, in any domain one may teach a doctrine that supports a given ideology but not the other way around. For instance, a Christian ideology may include a doctrine of social gospel but a social gospel without Christianity amounts to a form of social work. It is also true that the same doctrine can be used to serve multiple ideologies. For instance, the doctrine of popular sovereignty, *i.e.*, that the legitimacy of the state is created by the consent of the people, does not necessarily entail a democratic ideology since a dictator can claim to represent the will of the people. So too, a theocratic ideology may suppose that the rule of God passes directly to the people as opposed to a clergy person. In short, when working within the same ideology, it is the collection of doctrines that distinguishes different groups. To put the matter more concretely, the Sunni and Shi'a traditions are of the same ideology, which is Muslim, but they are marked by profound doctrinal differences. For instance, the Shi'a Imamite doctrine of *ijtihad* (interpretation) teaches that qualified jurists can render legal decisions on general principles found in the *Qur'an*. The Sunnite tradition, by contrast, bases decisions on the verdicts of earlier jurists.[8] This doctrinal difference does not, however, make either group less Muslim.

Although the concepts of doctrine and ideology are related through a one-way dependence, it is not the case that the relationship is causal. In other words, one can subscribe to a particular ideology and then learn the doctrines that support, explain, or confirm that ideology. For instance, one may be a proponent of a democratic ideology before understanding the doctrine of popular sovereignty. On balance, one can accept a doctrine but that doctrine does not serve as either the material or the efficient cause of an ideology. The truth is that the relationship between a doctrine and an ideology is more properly considered to be merelogical (part/whole relationship) in the sense that a doctrine is a part of an ideology. To put the matter more clearly, it might be useful to think of the relationship between doctrines and ideology as analogous to the points and lines that form a rectangle. In this case the rectangle is to an ideology what the points and lines are to doctrines. So, one may recognize the basic shape of a rectangle without knowing the exact coordinates for the points that determine the length and the width. Yet, the simple recognition of a rectangle does not change the fact that the points determine the size of the shape and that establishing one point is not sufficient for calculating the area of the rectangle.

The goal here is not to fully explore the part-whole relationship between doctrine and ideology. Rather, the aim is to draw out the notion that from a tactical point of view there are advantages to understanding the relationship. Most importantly, there is value in recognizing that by repositioning doctrines it is possible to change an ideology. Indeed, just as it is possible to change the area of a rectangle by changing the distance between the points, so it is possible to change an ideology by changing the doctrines. In a large alteration, the manipulation of doctrines can lead to the destruction of an ideology in the same way that dramatically rearranging the points would disassemble the shape. On a smaller scale, however, subtle or minor changes to a few doctrines that support an ideology can reduce the richness of the ideology. In a manner of speaking, manipulating a doctrine can be tantamount to changing the length and width of the rectangle while leaving the basic shape intact. So for example, within a fundamentalist movement like al-Qa'ida, one might extend Ibn Taymiyya's (1263-1328) doctrine of revealed truth in a way that not only supports his rejection of Aristotelian logic but also precludes the use of all tools that are constructed from Western logic such as the Internet. Extending the doctrine in this way is consistent

with one of al-Qa'ida's reasons for following Ibn Taymiyya – it is in line with the desire to guard against Western influences. Yet, by extending the scope of the doctrine the basic shape, *i.e.*, the puritanical ideology, is broadened to preclude mediums of modern communication.

A CAROLINGIAN TACTIC

Manipulating doctrine for combat purposes can be a subtle game but, regardless of the degree of change, the most effective alteration comes by leveraging doctrine in a way that is consistent with the existing belief system. This latter point is perhaps best illustrated through one strategy that the Frankish King, Charlemagne (768-814), employed in order to unite Western Europe under one crown. To be sure, the quelling of the Saxons serves as a case for the intentional manipulation of a doctrine in order to end an insurgency and defeat an ideologically motivated enemy. According to most general accounts, Charlemagne had repeatedly invaded and attempted to subdue the pagan Saxons during the years 772-785. Throughout the course of the campaigns the standard methods used to control conquered people, *e.g.*, forced oaths of allegiance, mass deportation, and the slaughter of prisoners, actually served to stiffen the Saxon resistance. Charlemagne eventually gained a few key military victories deep within Saxon territory and, rather than simply executing those responsible for the revolt as he had done earlier, he gave his enemies a choice to either accept the Christian rite of baptism or be slaughtered.[9] On the surface, participating in a church ceremony probably should not have carried any more weight with the Saxons than taking an oath. That is to say, for a non-Christian Saxon who had learned that religious-based oaths mollified the invader but were essentially meaningless to a non-believer, participation in a church ceremony should have held little sway. There is also evidence indicating that some Christian theologians also questioned the validity of the choice that was offered, a concern that Charlemagne ignored. Despite the apparent odds against success, however, the forced evangelization of the Saxons worked because their participation in the rite of baptism meant that they had formally joined Christianity. As an extra barb in the exercise, the Saxon participation in the ritual meant that they were disabled by their own definition of fidelity. They had abandoned their own faith tradition, engaged in a heresy according to the rules of their own religious system, and could no longer be emboldened by the belief that their insurgency would be supported through divine intervention. In short, Charlemagne attacked the Saxons at the center of gravity of their belief system and in doing so he opened the way for a new body of religious concepts that engendered political loyalty.

Just as religious belief had a center of gravity for the Saxons so it is with aberrant forms of Islam.

There are, in the example of Charlemagne and the Saxons, two key points worth noting. First, there is a tacit recognition that religious belief is a real and binding thing. To the extent that this applies to the modern conflict with Islam, the instructive element is that just as religious belief had a center of gravity for the Saxons so it is with aberrant forms of Islam. This aspect of religious faith is perhaps difficult for rationalistic minds to grasp because, as Bernard Lewis has rightly pointed out, Western history has consistently sought the "real" or "ultimate underlying" significance of religious conflict. Thus, it can be difficult to accept that people in other places actually do ascribe religious causes to religious movements.[10] The second key lesson is that the tactical use of doctrine is not equivalent to propaganda. Indeed, Charlemagne's example involves the legitimate construction of a scenario in which the enemy was disabled by its own definition of heresy as opposed to being misinformed. To be clear, propaganda is about the placement of information as a means for winning support or fomenting opposition rather than using a doctrine to render a religious movement inoperative. Hence, it is propaganda when the U.S.-born Anwar al-Awlaki uses sermons to actively call for war against American citizens. Presumably an appropriately propagandist response would be to link al-Awlaki to a controversial figure like Abdallah ibn Saba, the Jewish convert who allegedly remained loyal to his roots and attempted to destroy Islam from within.[11] Indeed, in propaganda the response only requires a competing message that discredits the opposition. It does not require the strategic deployment of religious doctrines.

THE DOCTRINAL CONSTRUCTION OF AL-QA'IDA

So far, two points have been made. First, I nailed my colors to the mast by asserting that a religious belief system is akin to an object that can be knocked off balance by striking a blow at the center of gravity. Second, the point has been made that Western approaches to the problem of Muslim extremism are often amiss because they address social concerns as opposed to doctrinal issues. That is to say, rather than simply accept religious fervor as an explanation for militant behavior many approaches seek deeper causes such as poverty or a failed secular state as the true issues. The practical strategies that result from these "discovered" explanations for radical behavior often involve attempts to win tribal favor through the promise of better local infrastructures such as schools, roads, and

police. Yet, it is precisely this approach and its outcomes that seem misplaced. The tactics are, admittedly, a politically important part of a successful campaign. Nevertheless, one must acknowledge that those same tactics are pre-set by the method. Consequently, if one takes seriously the proposition that an aberrant approach to religion is the cause of extremist behavior, it follows that tactics which are devised in response to social problems are misguided. Indeed, in working with an aberrant religious system the strike should be aimed at reducing the impact of the bad faith or triggering a faith crisis in its followers. This point has been strongly suggested in Colonel Brian Drinkwine's assessment of al-Qa'ida. As he would have it, the centripetal force is its ideology and the consequence of misreading that fact leads to attacking key functions such as leadership or funding that provide tactical gains but limited strategic victories.[12]

Given that terrorism is a tactic but theology is the tie that binds al-Qa'ida, there is value in contending seriously with Bruce Riedel's central thesis that challenging al-Qa'ida's narrative is critically important.[13] The caution in this, however, is that care must be exercised when punching at doctrines. Most obviously, the danger is that the general Muslim ideology incorporates some of the same intellectual components across a number of traditions; thus, attacking the wrong doctrine could result in widespread collateral damage. For instance, attacking ibn Taymiyya's contributions could have an adverse impact on any number of pietistic forms of Islam that stand in the Hanbalist tradition including the Wahhabism of Saudi Arabia and the Caucasus.[14] Despite this danger, however, it does make sense to start tapping on al-Qa'ida at the doctrinal level. To be sure, finding ways to reduce the area of the shape by working with the points and lines is a sensible strategy. Moreover, the doctrine of *jahiliyya* as it occurs in the later writings of Sayyid Qutb is a good candidate for the exercise. On the one hand, Qutb's doctrine is an attractive choice because of his place in history. He was an Egyptian struggling largely against the reign of Abdul Nasser (1956-1970). Thus, his historical proximity to al-Qa'ida suggests that his status in Islam is more akin to that of a cult hero than an intellectual patriarch. To put it bluntly, his ideas have not perdured so as to gain wide acceptance in the Muslim faith. On the other hand, the doctrine of *jahiliyya* is well suited to being manipulated in a way that forces al-Qa'ida to admit that it cannot have what it wants without being what it rejects. To put it more clearly, there are grounds for exploring whether or not al-Qa'ida can both have and sustain its desired, rigorous level of purity without an existing *jahili*.

QUTB'S DOCTRINE OF JAHILIYYA

To the best of my knowledge, the finest explanation of Sayyid Qutub's doctrine of *jahiliyya* has been provided by William Shepard. Indeed, Shepard has explained that the conventional use of the term *jahiliyya* is to translate it as "age of ignorance" and use it in reference to the period prior to Muhammad's mission. Moreover, Shepard notes that the root of the term does not connote "ignorance" *per se*. Rather, it suggests "barbarism" and the tendency to go to extreme behavior. In stark contrast to this conventional meaning of the term, Sayyid Qutb developed a new set of connotations in his commentary *Fi Zilal* and then popularized that new meaning through his last work *Milestones*. First, according to Qutb, *jahiliyya* suggests a rejection of divine authority in favor of human authority. Second, he shifted the meaning of the term from a period in time to a spiritual condition. Third, Qutb drew a strict dichotomy in which society is either *jahiliyya* or *Islam* and on the basis of that distinction judged the whole world as *jahiliyya*.[15] Although this highly stylized explanation of *jahiliyya* differs dramatically from the meaning of the term as it appears in the *Qur'an*, it is important to note that Qutb's commentary is not intended to be *tafsîr* (exegesis). As Olivier Carré has made clear in his initial observation, *Fi Zilal* is more of a militant meditation on the *Qur'an*.[16] The value in this observation is that Qutb's doctrine is an adaptation as opposed to an interpretation of the sacred text and, as such, it can be viewed as theologically tenuous. Further, because Qutb's recasting also animates some of the thinking in radical Islamic movements, it is a useful revision that can be targeted with limited risk of causing unwanted injury to the norms and customs of Islam.

That one can grasp an ideology without a full knowledge of the doctrines that make up a given system was mentioned earlier. It is a common-sense observation and, without argument, it also holds true for many members of al-Qa'ida and its associated movements.[17] That is to say, many of the people who join al-Qa'ida are capable of understanding the broader ideology of Global Islamism without having a detailed knowledge of the nuances that are associated with Qutb's doctrine of *jahiliyya.* Regardless of the level of technical knowledge, however, these people have a basic sense that their ideology entails a simple dichotomy, i.e., true Muslims versus the rest of the world. Such a partially informed view is extremely dangerous but it also breeds a kind of uncertainty that can be exploited. More precisely, if *jahili* (all societies that place authority in either other divinities or human institutions) were toppled, it does not follow that the people in those societies necessarily would "choose" to submit to God. In other words, the elimination of *jahili* does remove the overt signals by which submission is gauged. Nevertheless, the absence of visible alternatives

only implies that *Islam* is a matter of right behavior rather than an act of devotion to God proper. To be sure, there is a subtle but important distinction between acting *in accordance with* a rule and acting *because of* a rule. Qutb essentially acknowledged this in both the final chapters of *Fi Zilal* and in his general condemnation of Muslim society in *Milestones*. As he puts it:

> all the existing so-called "Muslim societies" are also *jahili* societies. We classify them among *jahili* societies not because they believe in other gods besides Allah . . . but because their way of life is not based on submission to Allah alone. . . .they have relegated the legislative attribute of Allah to others and submit to this authority, and from this authority they derive their systems, their traditions and customs, their laws, their values and standards, and almost every practice of life.[18]

In any religious system there simply is no way to discern when somebody's expression of faith is greater than empty conformity. It is precisely this limitation that breeds suspicion and often leads to schisms within religious movements....

Therefore, the problem, as Qutb sees it, is that the entire Muslim world essentially engages in confused acts of faith. Yet, even if the customs and laws were strictly aligned with dictates in the *Qur'an* it would still be impossible to gauge whether or not everyone has actually submitted to God. The truth is that in any religious system there simply is no way to discern when somebody's expression of faith is greater than empty conformity. It is precisely this limitation that breeds suspicion and often leads to schisms within religious movements and there is, even now, opportunity to raise questions about the level of *jahiliyya* existing within the ranks of al-Qa'ida.

Following on this notion, one might also note that the imposition of religious faith by force amounts to a direct contradiction of Qutb's argument, which is the absolute rejection of any society that accepts human authority over divine authority. That is to say, the revolutionary who brings about the change to global adherence to Allah by force is a human authority and the act of imposition, whether carried out by a divinely appointed agent or not, necessarily entails a power relationship in which one set of people dominates another. In a manner of speaking, sovereignty (*hakimiyya)* would be ascribed to and characteristic of the victorious militant force rather than to the divine. Without putting too fine a point on the matter, the militant force would be heretical in the sense that in removing the *jahili* it proposes to do what God either does not want or cannot do. The truth is that if one accepts Qutb's absolutist position that every society is *jahiliyya* and that the members of the militant sect come from those societies, then there is every reason to suppose that the revolution will bring about a new society that is also *jahiliyya*. Indeed, one might speculate that the fault in the new social movement would be conceit (*ghurur*), either because of the presumption to divine appointment or the blasphemous action of attempting to change a state of affairs that God had already determined. Simply put, Qutb did acknowledge that God's sovereignty consists both in his foreordaining of events and in his law. Yet, Qutb never seriously reckoned with the possibility that the *jahili* exist because God wants it that way.

SEEKING CHARLEMAGNE'S SOLUTION

Sayyd Qutb's doctrine of *Jahiliyya* may not be the center of gravity for al-Qa'ida. It is, nevertheless, an important doctrine in militant theology and misunderstanding that fact can lead analysts to create inaccurate explanations. For example, when Dennis Ross interpreted al-Qa'ida's justification for the deaths of non-combatants, he noted that senior leaders in the terror organization claim that individuals share an equal blame in the action of their governments. Thus, civilian deaths are justified because those people are equally responsible for the war.[19] In light of Qutb's doctrine of *jahiliyya*, however, it would appear that Dr. Ross has mistaken an "explanation" for a "justification." That is to say, al-Qa'ida explains that civilians are killed in acts of terrorism simply because there are no non-combatants. The justification or warrant for the killing, however, is grounded in a doctrine that calls for the destruction of all societies that do not conform to their version of Islam. One consequence in missing this nuance is that one can conclude, as Dr. Ross does, that many in the broader Muslim community accept the "charges and mythologies" of a group like al-Qa'ida because the narrative resonates with, for lack of a better term, a collective bad self-esteem. That is to say, Ross asserts that people in the Islamic world accept what al-Qa'ida is saying because they long for the greatness of the past, abide feelings of humiliation since World War I, and are angered by government corruption that is supported by the West.[20] It does not appear to occur to Dr. Ross that another reason why some Muslims accept the al-Qa'ida narrative is that it appears to be consistent with the larger ideological framework that constitutes Islam. It is by this same token that few Muslim leaders react when attacks are carried out against Israeli or Western targets. The victims are non-Muslims and, as such, the attack is not a Muslim problem. Nonetheless, if a

Sunni population suffers an attack, as Dr. Ross does point out, the reaction among Muslim people will be one of outrage.

The U.S. should ... work to create a climate that views both al-Qa'ida and its associated movements as apostate groups.

Although Dr. Ross appears to overlook the importance of religious doctrine, his analysis is instructive in one important respect: his study suggests that the broader Muslim world does not fully see itself as an enemy of al-Qa'ida. If that is accurate, then the point amplifies the general utility of Qutb's doctrine of *jahiliyya.* Indeed, that component part within the extremist theology does place most of the world, Islamic nations included, in the cross-hairs of al-Qa'ida. Many Muslim states, however, are merely a lower-priority target. The U.S. should take advantage of that fact and work to create a climate that views both al-Qa'ida and its associated movements as apostate groups. Expressed in theological terms, the U.S. needs to redirect the charge of *kafir* (non-Muslims and Muslims who purportedly hide or simply do not accept the realities of Allah's authority) back onto al-Qa'ida. This is important because, if the center of gravity for al-Qa'ida is a doctrine within its theology, as opposed to its leadership, the conditions for isolation and clear identification are prerequisite to any strategic victory. The truth is that any failure to underscore the point that attacks by al-Qa'ida are a step toward future assaults on Islam is a missed counter-strike in an ideological war. More frighteningly, because al-Qa'ida is allowed to continue to operate under the cover of the broader Islamic ideology, the failure of Muslim nations to grasp the larger significance of an attack as a step toward mainstream Islam tacitly implies a receptiveness to submit to al-Qa'ida's theological world view.

With that in mind, it is imperative that nations stop characterizing al-Qa'ida and its associated movements as sectarian, fundamentalist groups within Islam. Rather, al-Qa'ida should be recognized for what it is: a perversion of Islam. When this is done, pronouncements such as the fatwa against suicide bombing that was issued by Muhammad Tahir-ul-Qadri can be valued for more than their legal standing and the promise of slowing the radicalization process for new recruits. To be sure, there is no practical reason to think that an al-Qa'ida convert would accept Dr. Qadri's legal ruling regarding a particular tactic. There is every reason to think, however, that such pronouncements can be leveraged as a general defense of Islam against *kafirs*. This does not mean that the U.S. would somehow cede its military role in the problem. Far from it! The implication is simply that there is value in using *ijitihad* as a shield against adaptive theology, especially one such as Qutb's which has already been condemned.

Following Charlemagne's strategy, the aim here is to use doctrines in a way that both breaks al-Qa'ida from Islam and then forces it to crush under its own weight.

If one can take seriously the propositions that (A) al-Qa'ida theology is not Islam and that (B) everyone who does not share the al-Qa'ida theological world view is an enemy combatant, then the stage is set to begin exploiting Sayyid Qutb's doctrine of *jahiliyya*. To be sure, when introducing his doctrine, Qutb clearly stated that the group which will revive Islam must first completely separate itself from *jahili* society and become independent.[21] Coalition forces should take this literally. Every weapon, dollar, and communications route that is used by the terrorist organization illustrates the failure of al-Qa'ida to become independent of the very group that it opposes. This fact permits one to zero in on an important dichotomy that Mary Habeck identified: al-Qa'ida needs ordinary Muslims to join its movement but also demands religious purity that is extraordinary.[22] For Habeck, this dichotomy opens the way to rebrand the radical movement as *khawarij* (heterodox Muslims who, shortly after the death of Muhammed, claimed that they alone were the true believers). Such an opportunity for rebranding certainly does exist but, for combat purposes, the application is off target. On the one hand, ordinary Muslims may or may not grasp the nuances of early Muslim history and, on the other hand, pointing to a lineage may reduce the opportunity to sever the radical movement completely from its connection to the broader Islamic ideology. Indeed, following Charlemagne's strategy, the aim here is to use doctrines in a way that both breaks al-Qa'ida from Islam and then forces it to crush under its own weight. Slightly recasting Habeck's thesis then, the material connections that prove that al-Qa'ida is the form of *jahiliyya* that it detests both hangs the group on the horns of its own puritanical dichotomy and further confirms that the members of the group are themselves *takfiri* (apostates).

As noted above, attempts to discover the root cause that motivates people to join al-Qa'ida and its associated movements are likely misplaced. As such, checking the assessments of political scientists who locate the causes of terrorism in issues like poverty or a failed state is critically important. As Anthony Oberschall has explained, radical movements like al-Qa'ida are not concerned with the

failure to modernize. Rather, they are concerned with excessive modernization and the importing of Western ways to Muslim people. What this means is that al-Qa'ida is concerned with a deep desire to not be like the West. Simply put, the people who fight for al-Qa'ida operate within a doctrinal framework in which they are convinced that they are aspiring to a hazy notion of what they think is better. Hence, it follows that promoting democracy, nation building, etc., are like spicy food on an ulcer. They are an irritation on a pre-existing condition that causes a flare-up. Naturally, it is not possible to account for all of the individual reasons that drive people to terrorism. As Jessica Stern rightly noted, "the reasons that people become terrorists are as varied as the reasons that others choose their professions."[23] Yet, once people join a group like al-Qa'ida, the doctrinal construction of the movement serves as a collection point for the aggrieved and provides them with the justification to act out aggressively. As Professor Stern's anecdotal evidence suggests, however, the religious ideology can be reformed through an educational process of religious instruction. Yet, rather than reprogram the individuals who take up terrorism in the name of an ideology, it makes more sense to reprogram the ideology itself. Indeed, for those who remain in al-Qa'ida, the blind spot of ignorance will continue to be one of the greatest vulnerabilities.

RECOMMENDATIONS

Given that the center of gravity for al-Qa'ida is likely a religious doctrine, a process should be engaged that involves disassociating the aberrant militant ideology from the normal religious ideology of Islam.

1. In order to attack a militant belief system at its center of gravity, the first step must be a review of the DOD Joint Publication (JP) 5-00.1, *Joint Doctrine for Campaign Planning*. It is in that document that the current military definition of a center of gravity is nuanced in ways that differ from the concept as initially put forward by the Prussian strategist Carl von Clausewitz. While the Joint Chiefs' statement and ensuing calculus for finding the center of gravity is a model of efficiency, it is not particularly helpful in the case of al-Qa'ida. There is value in simplifying the basic metaphor of applying a geometric property to an object such as a military force, nation, or religious group. Just as different physical objects such as statues and airplanes have different centers of gravity so it is that different abstract objects have different centers of gravity. The metaphor for a center of gravity is to suggest that one should locate the point (not the source of power) at which the weight of that particular object is concentrated. To the extent that this applies to a religious group like al-Qa'ida, the inference is that the greatest concentration of weight that holds the object in balance will be a religious doctrine.

2. Given that the center of gravity for al-Qa'ida is likely a religious doctrine, a process should be engaged that involves disassociating the aberrant militant ideology from the normal religious ideology of Islam. This can be accomplished by taking account of the various sources that combine to make al-Qa'ida's belief system. Once that is done, it makes sense to inventory key doctrines that have special significance for al'Qa'ida and, as a consequence, bear the weight of the militant ideology. There may also be some utility in forming a cross-disciplinary team that involves war planners, intellectual historians, and professional theologians (not clergy) who can work together to assess the various doctrines for their value as a center of gravity. The rationale for this is that having a list of available doctrines is not sufficient. In order to short-circuit the ideology one must know how the various doctrines work within the theology.

3. Al-Qa'ida is currently an international organization. As long as its ideology remains in its current form, it can continuously adapt and flourish much as a Christian organization can exist under a centralized structure, e.g., the Vatican, or under a decentralized model, *inter alia* the Church of Christ. That is to say, as long as the basic ideology remains undisturbed, the religious movement will continue to adapt. There is, however, an opportunity to knock al-Qa'ida or one of its associated movements off balance by manipulating doctrines in order to create, for lack of a better term, interdenominational strife. Thus, the U.S. and its partners should work to exploit the linkages between al-Qa'ida and its allies but use the organization's own standards of purity to drive a rift.

Although Charlemagne's tactic involves trapping an enemy in its own ideology, one should not overlook the value of propaganda.

4. Although Charlemagne's tactic involves trapping an enemy in its own ideology, one should not overlook the value of propaganda. The aim of that propaganda, however, should hit two targets. First, the U.S. and its allies should make greater use of events such as the 2004 Riyadh bombing that was carried out by al-Haramain. Such events help to better communicate that al-Qa'ida regards the diversity within Islam as an enemy, serves to

embolden Muslims against the militants, and helps to focus American sympathies. Second, to the extent that the propaganda should be aimed directly at al-Qa'ida, there is tremendous value in working to discredit the religious movement as a whole. Focusing on messages that include bin Laden's faulty, albeit effective, use of the Crusades or his dispirited warning to his son helps to reduce his iconic status. Nevertheless, it is important to distinguish between messages that suggest that he is a rebel headed toward martyrdom and those that portray the entire movement as a pseudo-faith. [Editor's Note: This article was submitted before the May 2011 takedown of bin Laden's compound and his death.]

CONCLUSION

To the best of my knowledge, it has been just over one thousand years since any major power seriously treated religious doctrine as an enemy's center of gravity. With that in mind, the strategies of those who were more closely acquainted with the tactic, *inter alia* kings such as Charlemagne and his father Pippin, may be instructive for finding the most expeditious way to destroy the conceptual framework through which a modern, aberrant, Muslim insurgency continues its work. In his own right, Charlemagne's tactics were close to barbarian forms of warfare in the sense that human rights and politically correct sensitivity for other religions really were not a concern. Rather, there is in Charlemagne's war-craft a sense that what mattered was discovering how to bring his conflicts to a decisive point. What this meant for Charlemagne was that religion was a tactical weapon, clergy members were a propaganda device, and brutal intolerance was the response for any loss on his side.

Charlemagne's counsel to modern war planners would be to gain public opinion, including that in the Muslim world, and then attack al-Qa'ida at the doctrinal level of its theology.

These are unpleasant aspects of his strategy. Nevertheless, what distinguished Charlemagne from earlier barbarian kings was his profound ability to deploy these tools in a way that was both careful and calculated. In this sense, Charlemagne is not too far from Clausewitz in supposing that the direct annihilation of the enemy's forces is the dominant consideration and that even moral sentiments factor into that goal. To the extent that this applies to an adversary like al-Qa'ida, there is already evidence that it can adapt and change strategies in order to sustain its religious war. Thus, one might suppose that Charlemagne's counsel to modern war planners would be to gain public opinion, including that in the Muslim world, and then attack al-Qa'ida at the doctrinal level of its theology.

Notes

[1] S. Pelletiere, "A Theory of Fundamentalism: an inquiry into the origin and development of the movement," Strategic Studies Institute (1995), p. 39. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubid=195 Accessed: 2-19-2010

[2] K. Siqueria, "Political and Militant Wings within Dissident Movements and Organizations," *Journal of Conflict Resolution*, v. 49, no. 2. *The Political Economy of Transnational Terrorism* (April 2005), pp. 218-236.

[3] H. Ansari, "The Islamic Militants in Egyptian Politics," *International Journal of Middle East Studies*, vol. 16, no. 1 (March 1984), p. 123.

[4] C. Fettweis, "Freedom Fighters and Zealots: Al Qaeda in Historical Perspective," *Political Science Quarterly*, v. 124, no. 2 (2009), p. 270.

[5] See, for example, J. Ethridge, "Center of Gravity Determination in the Global War on Terrorism," USAWC Strategy Research Project, U.S. Army War College (2004).

[6] B. Head, *Ideology and Social Science: Destutt de Tracy and French Liberalism* (Dordrecht, 1985), p. 32. See also E. Kennedy, *A Philosophy in the Age of Revolution: Destutt de Tracy and the Origins of "Ideology"* (Philadelphia: American Philosophical Society, 1978).

[7] D. Meghnad, *Rethinking Islamism: The Ideology of the New Terror* (New York, 2006), pp. 23-25, 59.

[8] W.M. Watt, *Islamic Philosophy and Theology* (Edinburgh, 1992), p. 151.

[9] R. Collins, *Charlemagne* (Toronto, 1998), pp. 47-57. R. McKitterick, *The Frankish Kingdoms under the Carolingians* (London, 1983), pp. 61-63.

[10] B. Lewis, "Some Observations on the Significance of Heresy in the History of Islam," *Studia Islamica*, no. 1 (1953), p. 44.

[11] B. Lewis, "Some Observations," *Studia Islamica*, no. 1 (1953), p. 44. For a brief reference of ibn Saba's discord, see M. Fakhry, *A History of Islamic Philosophy* (New York, 1983), p. 56.

[12] B. Drinkwine, *The Serpent in our Garden: Al-Qa'ida and the Long War*, Strategic Studies Institute (January 2009), p. 26.

[13] B. Riedel, "Obama's War: Prospects for the Conflict in Afghanistan and Pakistan," *The Afghanistan Papers*, no. 7 (September 2010), p. 7.

[14] On Wahhabism as a form of fundamentalism in the former Soviet Union, see A. Knysh, "A Clear and Present Danger: 'Wahhabism' as a Rhetorical Foil," in *Die Welt des Islams*, New Series, v. 44, no. 1 (2004), pp. 3-26.

[15] W. Sheppard, "Sayyid Qutb's Doctrine of Jahiliyya," *International Journal of Middle East Studies*, v. 35, no. 4 (November 2003), pp. 524-525.

[16] O. Carré, "Eléments de la 'alqîada de Sayyid qutb dans Fî Zilâl al-qur'ân" *Studia Islamica*, no. 91 (2000), p. 168.

[17] On this point see J. Stern, "Mind over Martyr: How to deradicalize Muslim extremists." *Journal of Foreign Affairs* 89, 1 (January-February 2010), pp. 97-98.

[18] S. Qutb, *Milestones*, American Trust Publications (2005), p.61.

[19] D. Ross, "Counterterrorism: A Professional's Strategy," *World Policy Journal* (Spring 2007), p. 19.

[20] D. Ross, "Counterterrorism," pp. 21-22.
[21] S. Qutb, *Milestones*, American Trust Publications (2005), p. 32.
[22] M. Habeck, *Knowing the Enemy: Jihadist Ideology and the War on Terror* (New Haven, 2006), pp. 166-167.
[23] J. Stern, "Mind over Martyr: How to deradicalize Islamist extremists," *Foreign Affairs* 89, 1 (January-February 2010), p. 97.

J.A. Sheppard is Vice President of Academic Affairs at Southwestern College in Kansas. He studied the history of Islamic philosophy while working toward his master's degree at the Iliff School of Theology in Colorado. He then earned a PhD from the University of Sheffield, England, where he wrote about the theory of names according to John Duns Scotus. He is the author of Christendom at the Crossroads. *Specializing in the history of ideas, he has written articles related to medieval philosophy and academic leadership. He has also served as an invited speaker in support of educational programming for both the Army and the Air Force. His lecture, "1095: Origins of the Long War," contrasted the Crusades with the current conflict and was delivered as part of a guest speaker series at McConnell AFB, Kansas, in 2007.*

Cyber Threat Assessments:
A New Tradecraft Paradigm

by Dr. Christian Hirst and Mathew "Pete" Peterson

EXECUTIVE SUMMARY

Cyber security's emergence as a central national security concern for modern Western states requires the intelligence communities of these states to ensure they are providing balanced and holistic assessments of the nature of cyber threats. To avoid the risks associated with misleading, overly technical, or misinformed assessments of the cyber threat, this article posits that a unique cyber threat assessments tradecraft paradigm is required. Such a paradigm needs to be interdisciplinary in nature, and underpinned by the integration of the technical and strategic skill sets required to provide cyber threat assessments that can effectively inform proactive and comprehensive cyber security strategies.

This new paradigm would replace previous analytical approaches that witnessed groups of technical analysts independently focusing on the technical level and non-technical analysts independently focusing on the strategic/behavioral elements of cyber threats. The authors argue that a useful starting point would be to learn the lessons of the Australian Cyber Security Operations Centre (CSOC), which has seen some early successes in developing such a paradigm through collocating technical specialists and generalist intelligence analysts in the same operations centre.

THE EMERGENCE OF CYBER THREATS AS A NATIONAL SECURITY CONCERN

For modern Western states, cyber security has rapidly emerged as a top-tier national security issue. There has been a growing recognition among national security decision-makers in these states of their society's, economy's, and military's dependence on "digital infrastructure" and the vulnerability of this infrastructure to cyber threats. The increasing resources that Western states are dedicating to cyber security are also a result of transformations in the nature of the 21st century state and an ongoing reorganization of the principles that underpin these post-industrial societies.

As Phillip Bobbit (2002) has pointed out, the legitimacy of modern Western states is now less dependent on defending territorial borders and providing public welfare and more reliant on protecting the lives of individual citizens – whether at home or abroad – and maximizing each citizen's opportunities and access to the choices markets provide. Bobbit defines this as the shift from nation states to market states. A central enabler and driver of the transformation of the state has been the information and communications technology (ICT) revolution. Therefore, threats to the enabling characteristics of information technology networks are also to be conceived of as threats to the legitimacy of the modern 21st century market state.

Manuel Castells' (1996) theory of the network society provides further context to the increasing importance of ensuring the integrity of information and communications networks. Castells argues that the information technology revolution has reordered the principles that underpin social interactions. As industrialized capitalism created societies characterized by hierarchy and mass political and social movements, the ICT-enabled, post-industrial society is defined by structures and activities organized around electronically processed information networks (Castells, 1996). To be sure, Castells' network society is not just a technological conception; it also describes the organizing principles that shape political, religious, and cultural interactions which occur within the network society. It is therefore unsurprising that the leaders of modern market states operating within the context of network societies are increasingly aware – either intuitively or explicitly – that threats to the integrity of the ever-expanding digital infrastructure which underpins the social and economic lives of their citizens are in fact threats to both the legitimacy of market states and the fabric of networked, post-industrial societies.

ATTRIBUTION AND THE NEED FOR A HOLISTIC APPROACH

Although networked market states are vulnerable to threats to the integrity and functionality of digital networks, clear and balanced assessments of the nature of the threats to these networks are critical to

ensuring that proactive and proportionate responses are undertaken. Overstating the threat, and responding disproportionately, could lead to a wide range of unintended consequences – including the needless militarization of cyberspace – which in itself will pose an even graver threat to the long-term integrity and functionality of digital networks. Therefore, as cyber threats and cyber security increasingly command the attention of senior decision-makers, it is the responsibility of the Intelligence Community to provide balanced and holistic assessments of the threats posed to the digital networks that are critical to both the functioning of society and the legitimacy of the state.

In defining the nature of the cyber threat, the critical task confronting intelligence professionals is identifying the source of offensive cyber activity and the intentions behind such activity. The traditional approach to analyses of network events/intrusions involves two separate, yet often parallel, efforts to analyze data associated with these events. We shall call this our "Coin" analogy. The analysis of technical behaviors associated with the incident ("Incident A") draws on the data supporting the "how, what, when, and where" elements of the incident – "It's a 'head' (hardware, firmware, software)." The analysis of social behaviors associated with the incident draws on the data supporting the "who and why" elements of the incident – "It's a 'tail' (education, training, preferences, languages)." Although both analytic efforts draw from the same overall set of data associated with Incident A, their efforts are often conducted in complete isolation from each other. This can result in incomplete or incorrect mitigation or attribution efforts.

Reactive, tactical mitigation does not require attribution. Cleaning up malicious software and updating and improving cyber security postures are a central element to increasing the costs for offensive cyber actors. However, over the longer term, the offense will always have the advantage over the defense's ability to adapt and respond to these events. Therefore, tactical/technical mitigation efforts must occur in concert with broader proactive defensive strategies that take into account the intentions and broader behavioral characteristics of the offensive cyber actors.

Highlighting high levels of malicious activity does not tell us that a threat is of a strategic nature. Active and deliberate campaigns on the part of political actors known to be hostile to the strategic preferences or objectives of the target require a more urgent and risk-tolerant approach to cyber defense than does defending against financially-motivated spamming activity, which requires a more deliberate public education campaign. Essentially, cyber threat analysts must not just assess the location and sophistication of each piece of detected offensive cyber activity, but also be able to determine the purpose and the strategic implications of the activity. Technical behaviors and social behaviors alike must be assessed in a holistic, or interdisciplinary, fashion.

A THEORETICAL FOUNDATION FOR HOLISTIC ATTRIBUTION

We submit that a holistic approach to these cyber analytic efforts represents an initial paradigm shift, as the data being analyzed are quite literally "all the same coin," whether the data represent technical, social, or techno-social behaviors. In his discussion of paradigms and paradigmatic change within communities, Thomas Kuhn notes that often it is times of crisis that result in the casting aside of former models and approaches that result in these paradigm shifts (1996, 3rd ed.). Previously-isolated approaches to conducting analyses of network events have been overcome by a need for holistic analytic approaches in an interdisciplinary manner.

The traditional approach to intelligence analysis and threat assessments – assessing the veracity of sources, synthesizing a variety of data inputs, ascertaining the capability and intentions of an adversary, and making forward-looking judgments of the threat – is not sufficient for a cyber analyst. Cyber analysts will rarely know the source of offensive cyber activity and need a broad base of general knowledge to assess the likely strategic objectives driving a certain grouping of cyber operations or events. In addition to this broad base of general expertise, they also need a solid grasp of the key technical elements that make up offensive cyber activity. Cyber analysts need to be agile in their understanding of human behavior; a certain stream of offensive cyber operations may seem consistent with a known adversary's technical modus operandi but the targeting and timing could indicate that a new or unexpected adversary is undertaking denial and deception through imitating another's techniques. The ease with which offensive cyber actors can obfuscate their activities puts a premium on agile strategic thinking for cyber analysts.

This argument for a "holistic attribution" approach is based on the concept of an interdisciplinary approach to analysis of these events. Dr. Michael Seipel writes on the subject of interdisciplinary analysis in an article about these approaches in the curriculum at Truman State University (2002). It is his definition of "interdisciplinary analysis" that is considered here, however:

> Interdisciplinary analysis requires integration of knowledge from the disciplines being brought to bear on an issue. Disciplinary knowledge, concepts, tools and rules of investigation are considered, contrasted, and combined in such a way that the resulting understanding is greater than simply the sum of its disciplinary parts (p. 3).

Why this focus on an interdisciplinary approach to the analysis of network events? If we return for a moment to Castells' theory of network society, we recall he theorizes that network society is comprised of both the technical network and the social network simultaneously (1996, 2000a, 2000b, 2000c, 2004). Therefore, analysis of network events focusing on only one or the other of the network aspects represents an incomplete analysis of the event. An interdisciplinary approach from the beginning of the analysis should result in greater synthesis of all of the analysis conducted, with a greater chance of attribution of the event.

Unlike traditional intelligence analysts, a cyber analyst needs an understanding of the vulnerabilities of systems of national interest. Rather than outside-in – e.g., "How will Iran's developing a nuclear weapons capability affect security in the Middle East and Western interests in the region?" – a cyber analyst must think inside-out – "How vulnerable are our critical national infrastructures and systems of national interest to cyber exploitation and attacks?"

A NEW TRADECRAFT PARADIGM

The tradecraft required to perform effective cyber analysis is, in many ways, the reverse of that reflective of a traditional intelligence analyst. It requires a broad base of general knowledge *and* narrowly focused technical knowledge. The assessment of threats must start from an understanding of internal vulnerabilities and project outward to a grasp of current and potential adversary capabilities, finally using an understanding of an actor's strategic objectives and behavioral preferences to determine intent. Therefore, a cyber analyst must be capable of assessing vulnerabilities and determining the implications of both human behaviors *and* technical behaviors.

Lastly, partnering and collaboration are central to the work of a cyber analyst. The wide variety of actors and the fast-changing nature of tactics and techniques require a cyber analyst to develop strong working relationships with technical, geographic, and thematic subject matter experts. Cyber analysts cannot be experts on the current intentions of every terrorist group, criminal entity, and state on the planet, but they can develop a strong network of relationships with those who are. When developing an understanding of internal vulnerabilities, again it is beyond the capabilities of a group of intelligence analysts to develop a comprehensive understanding of the vulnerabilities of each network that supports critical infrastructures or other systems of national interest. Here, partnering with the private sector, lower echelons of government, and non-traditional partners at the federal level is essential to gaining this appreciation of internal vulnerabilities and assessing the potential targets of adversaries.

The Australian government's recently launched Cyber Security Operations Centre (CSOC) – based within the Defence Signals Directorate – is an example of a capability designed to assess both the strategic and technical elements of offensive cyber activity. The CSOC was formally launched by the Australian Defence Minister in January 2010 and has been tasked with providing the government with a comprehensive understanding of cyber threats against Australian interests. It also is expected to coordinate and assist operational responses to cyber events of national importance across government and critical infrastructure.

In undertaking these roles the CSOC has developed close partnerships with key agencies across government, including the Australian Federal Police, the Australian Security Intelligence Organization, the Attorney General's Department, and the Strategic Policy Division of the Department of Defence. Nevertheless, the deepest and most successful partnership the CSOC has established to date has been with the Department of Defence's lead all-source strategic assessment agency – the Defence Intelligence Organization (DIO). Generalist DIO officers are fully integrated into the CSOC's Threat Assessment Section and have developed close working relationships with the significant technical expertise resident in the Defence Signals Directorate.

The collocation of all-source strategic analysts, technical experts, and traditional signals analysts has moved the CSOC some way toward developing the new paradigm of analysis outlined above. All-source generalists – through regular contact with technical analysts – are developing a strong base of technical skill, while technical analysts through conversations and discussions with the more strategically-oriented DIO analysts are developing a more nuanced appreciation of the factors that influence intent when analyzing technical data. To

be sure, the CSOC remains a nascent capability; DIO's integration and efforts to develop a new paradigm of analysis will require strategic and technical analysts to continue to respect and value each other's unique skill-sets and to maintain a commitment to collaboration and cooperation.

CONCLUSIONS/RECOMMENDATIONS

21st century challenges require 21st century responses and this is no less true in the cyber domain than in any other. In order to best achieve the new paradigm outlined herein, old approaches of analysis of ICT-related intrusions and attacks must be set aside in favor of interdisciplinary team approaches. By collocating technical analysts with general intelligence analysts, functioning as integrated "cyber analysis teams," a greater understanding of the nature and origin of these cyber threats can be gained.

This interdisciplinary team approach, in a foundational sense, can be furthered by training and education within and through private and public industries, academic institutions, governmental agencies and organizations, and international partnering efforts. Interdisciplinary, holistic approaches are the new paradigm, the appropriate response for modern states and the ICT-based threats they face together in the 21st century.

References:

Bobbit, Philip. 2002. *The Shield of Achilles: War, Peace and the Course of History*. Knopf, New York.

Castells, Manuel. 1996. *The Rise of the Network Society*. Wiley, San Francisco.

——. 2000. Materials for an explanatory theory of the network society. *British Journal of Sociology, 51*(1), pp. 5-24.

——. 2000. Towards a sociology of the network society. *Contemporary Sociology,29*(5), pp. 693-699.

——. 2000. Informationalism, networks, and the network society: a theoretical blueprint. *The Network Society – A Cross-cultural Perspective* (pp. 3-45). Edward Elgar, Cheltenham.

——. (ed.). 2004. *The Network Society: A Cross-Cultural Perspective*. Edward Elgar, Cheltenham.

Kuhn, Thomas. 1996. *The structure of scientific revolutions* (3rd ed.). University of Chicago, Chicago.

Seipel, Michael. 2002. *Interdisciplinarity: An Introduction*. Truman State University, Missouri.

Dr. Christian Hirst is the Director of the Australian Cyber Security Operations Centre's Threat Assessment Team. Prior to joining the Centre, he was a senior analyst with the Defence Intelligence Organisation's Combating Terrorism Section. Before joining the Australian Department of Defence, Dr. Hirst completed his PhD at the University of Queensland, where he analyzed the effects of September 11 on Australia's defense and foreign policy posture. He has published articles in a variety of academic journals, including The Australian Journal of International Affairs *and* The Australian Army Journal.

Mathew "Pete" Peterson has served in a variety of positions within U.S. government agencies since 1989, to include 13 years on active duty in the U.S. Army. He has experience in a wide range of domains, including information assurance/information protection; research, development, and acquisition (RDA)/research and technology protection (RTP); cyber analysis issues; critical infrastructure protection; and threat analysis. He currently serves as chief of the Cyber Analysis Division within the Naval Criminal Investigative Service, while working toward completion of his dissertation in the Executive Leadership Doctoral Program at George Washington University's Virginia Campus. Mr. Peterson authored an article in the Fall 2009 issue of AIJ *titled, "Organizational Leadership in the Intelligence Community: A New Paradigm."*

Risk-Based Cybersecurity Policy

by John G. Schwitz

OVERVIEW

"Understand, detect, and counter adversary cyber threats to enable protection of the Nation's information infrastructure" is one of six Mission Objectives stated in **The National Intelligence Strategy** [1].

This article demonstrates that the magnitude of the threat, ineffective defense, and current policies place U.S. infrastructure at extreme risk. It recommends two counterintelligence actions: **tracking-attribution** and **active-countering**, which deter and eliminate threats.

The article further develops the actions, process, and technology from three intelligence assessments:

(1) A ***risk assessment*** of infrastructure under attack,
(2) ***Threat capabilities***, particularly **surprise-in-force**, and
(3) ***Expected responses*** of adversaries to current U.S. cyber policies.

INTRODUCTION

The paper addresses the National Security Risk from growing threats to the Internet, telecommunication networks, and the electric grid. The paper proposes policies and actions by diverse parties in the Intelligence Community, DoD, Government, and private sector to mitigate this threat. The range of actions, in increasing order of effectiveness, are: ***Protect, Detect, Deter,*** and ***Eliminate.*** I demonstrate that the present government policy of ***defend-only (Protect)*** is failing to safeguard vital U.S. interests. I recommend two counterintelligence actions: ***tracking-attribution***, and ***active-countering***, which are biased toward ***Deter*** and ***Eliminate***. Actions to mitigate or eliminate threats require a combination of both actions. ***Tracking-attribution*** develops the source, capabilities, and other possible exploits of the threat. ***Active-countering*** uses this information to mitigate or eliminate the threat. These recommendations are consistent with the major goals and initiatives of The Comprehensive National Cybersecurity Initiative [2], Initiative #10:

> **Initiative #10. Define and develop enduring deterrence strategies and programs.** Our Nation's senior policymakers must think through the long-range strategic options available to the United States in a world that depends on assuring the use of ***cyberspace***. To date, the U.S. Government has been implementing traditional approaches to the cybersecurity problem—and these measures have not achieved the level of security needed.

Formulating effective policy includes ***quantifying risk*** and ***evaluating policy options***. This introduction develops the approach used throughout the paper. Effective intelligence shapes policy through quantifying risk by evaluating the causal chain of threat, vulnerability, and impact while discovering mitigating factors. The heuristic Risk Management equation relates these factors.

$$\text{Risk} = ((\text{Threat} \times \text{Vulnerability})/\text{Mitigation}) \times \text{Impact}$$

Figure 1: Heuristic Risk Relationship

This relationship illustrates the strong correlation between a threat, vulnerability, mitigation, and impact. A threat exploits a system vulnerability resulting in an impact (negative consequence). Once a threat or vulnerability is discovered and understood, the search for mitigating actions can be prioritized by the magnitude of the negative impact.

The paper quantifies infrastructure risk under attack, assesses threats from adversaries, and uses game theory to predict the reactions of adversaries to U.S. actions and policies. I conclude that the current U.S. cyber policy of ***defend-only*** elicits an optimal strategy from adversaries of ***attack***. Additionally, a ***defend-only*** cyber posture has a multiplier effect on adversaries' attack capabilities.

I quantify the risk on infrastructure using methods of self-organized criticality (soc), also called chaos theory, small world networks, or complexity theory. Findings from this work characterize the Internet, telecommunications, and

the power grid as susceptible to catastrophic failure from attacks. I then address mitigating actions countering these risks.

I evaluate policy efficacy using game theoretic methods pioneered by John Nash, elegantly applied to Cold War nuclear strategy by Thomas Schelling, and to conflict by Roger Myerson. All three were awarded the Nobel Prize in Economics for their contributions. This approach offers insight into an adversary's expected response to U.S. actions. This insight permits policymakers to evaluate the consequences of a wide range of prospective actions, thereby shaping policy toward desirable outcomes.

RISK ASSESSMENT

Attacks on critical nodes of U.S. infrastructure can lead to catastrophic failure. The robustness of this infrastructure to random failures lulls us into a false sense of security.

I quantify the risk on infrastructure using methods of self-organized criticality (soc). Self-organized criticality has modeled domains as diverse as earthquakes, forest fires, traffic congestion, and large disturbances in the power grid and the Internet. This work can also explain the rapid transmission of biological and computer viruses, diseases, and fads. Large empirical studies have validated this work. Findings from this work characterize the Internet, telecommunications, and the power grid as susceptible to catastrophic failure from attacks. This paper uses the term *infrastructure* to encompass the Internet, telecommunication networks, and the electric grid. From the May 2009 Cyberspace Policy Review [3]:

> National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) defines ***cyberspace*** as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

Can we quantify the risk to infrastructure? Is there empirical evidence justifying infrastructure risk? Can we mitigate the risk to infrastructure? I draw on a series of papers co-authored by Albert-Laszlo Barabasi to answer these questions in the affirmative [4],[5],[6]. The basic idea is that certain structures evolve through internally and externally driven processes toward a critical state. There is no architect or master plan. There is no reductive physics explaining the process. The differentiating feature of a critical state is its response to disturbances. A normal state responds, within a narrow range, with a characteristic response time and scale. A critical state is scale-free. It responds to disturbances with time and scale responses of any size. Most importantly, a Power Law describes the scale of response statistically. The Power Law models the frequency of an event to the scale (size) of the event.

Figure 2 describes key characteristics of a Power Law. Extensive empirical analysis reveals that Power Laws describe the responses of the Internet, telecommunications, and the electric power grid to disturbances.

A Power Law expresses the probability (y) of an event of magnitude x (x)

as: y = Probability {Event of magnitude = x} = x^{-k} hence;
a power law with exponet -k

taking the log on both sides transforms this to a linear equation:

Log[y] = -k Log[x]

The linear equation plots Log[y] against Log[x] with slope -k

Figure 2: Characteristics of a Power Law

Figure 3 demonstrates that the Internet backbone scales as a power law. The heart of the Internet, the Internet backbone, is the routers and links owned and operated by major providers such as AT&T, Sprint, and XO. The backbone routers are concentrated in certain locations and support 291,000 backbone IP addresses in the U.S. *Figure 3* from "Criticality analysis of Internet infrastructure" [7] plots the exponential relationship between the frequency {y axis} versus degree connectivity {x axis} on a log/log chart. The frequency captures the percentage of routers connected to x or more routers (degree connectivity). The chart displays the wide dispersion of router connectedness. 99% of the routers are connected to 50 or less routers. However, the remaining 1% of the routers are connected to a wide range of routers up to a maximum of 11,000 (arrow).

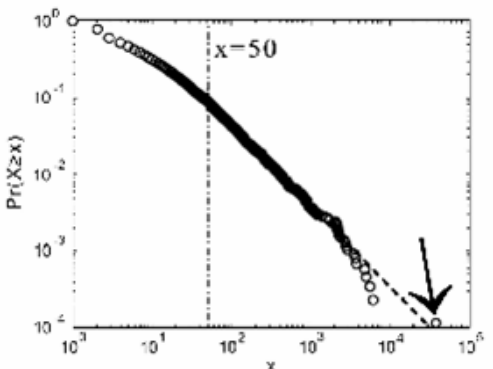


Figure 3: Distribution of Backbone Routers [7]

It's tough to make predictions, especially about the future …

This quote attributed to both Yogi Berra and the famous physicist Niels Bohr cleverly abstracts attributes of this relationship (self-organized criticality). The problem domain is non-linear, meaning that small disturbances targeted at critical nodes (high degree connectivity) can have extraordinary effects.

What justifies the terms "catastrophic failure" and "extraordinary effects" used to describe disturbances to infrastructure characterized by the Power Law? Power Laws have infinite variance. Operationally, this means many extreme events. Risk Managers use sophisticated techniques to quantify risk using the Normal Distribution, "fat-tailed" distributions, and Monte Carlo simulations. Extreme events (fat tails) are the cause of numerous "unexpected" catastrophes, because models were constructed improperly from the Normal distribution.

John Kay of the Financial Times captures this problem in his column on the Financial Crisis [8]:

> When the financial crisis broke in August 2007, David Viniar, chief financial officer of Goldman Sachs, famously commented that 25-standard deviation events had occurred on several successive days. If you marked your position to market every day for a million years, there would still be a less than one in a million chance of experiencing a 25-standard deviation event. None had occurred. What had happened was that the models Goldman used to manage risk failed to describe the world in which it operated.
>
> If the water in your glass turns to wine, you should consider more prosaic explanations before announcing a miracle. . . . .
>
> The source of most extreme outcomes is not the fulfillment of possible but improbable predictions within models, but events that are outside the scope of these models.

As Risk Managers we must capture elements of the real world – even if not yet observed – in our models. This paper achieves this through two approaches: (1) ***differentiating the effects on a network of directed attacks from random failures***, and (2) ***analyzing how U.S. Cyber Policy influences the actions of adversaries***. First, I address the effects of directed attacks versus random failures.

It is not possible to contain risk on a Power Law distribution: the tail events are too frequent and extreme. *Figure 4* demonstrates the number of extreme events in a Power Law. The chart plots log(probability) against log(event size) for Normal[1] and Power Law distributions. The area under the Normal distribution curve up to 1 standard deviation (event size of 9) represents 68% of the distribution. The area up to 3 standard deviations (event size of 25) represents 99.7% of the distribution. Contrast this with the Power Law; 5% of distribution has event sizes over 20 and 1% of the distribution has event sizes over 50. A Power Law is a different beast because it has infinite variance.

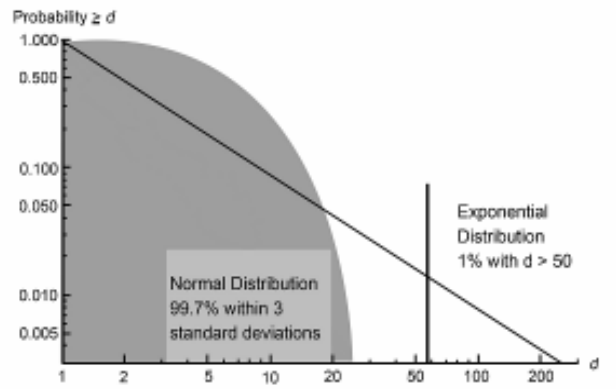


Figure 4: Extreme Events for a Power Law

Now the paper summarizes the empirical findings of catastrophic risk poised by Power Law relationships for the power grid and Internet backbone. Carreras et al. validated the Power Law, *Figure 5*, for all power transmission blackouts in North America from 1984 to 1998 [9]. The k factor (exponent) for blackouts is -1.1. This relationship means that there are many large blackouts. A k factor of -1 implies 10 times the blackout size; it only reduces the probability of occurrence by 1/10. Arrow 1 has 10 occurrences shedding 1/100 of total U.S. power. Arrow 2 (10 x the power shed of Arrow 1) has 1 occurrence shedding 1/10 of total U.S. power.

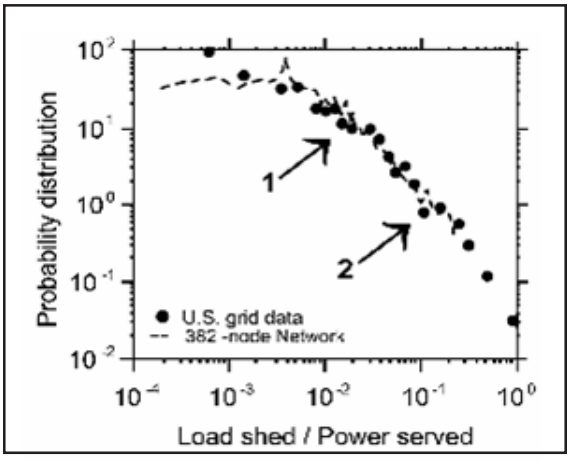


Figure 5: Blackout Probability vs. Blackout Size [9]

[1]Two times the (x>=1) segment of a Normal Distribution with

Similar results could be demonstrated for Internet and telecommunications. Albert et al. [5] model the network topology and dynamic behavior of scale-free networks. The term "scale-free" characterizes the ability of the networks to operate at immense scales and the dominance of a small number of nodes. The Internet, telecommunications, and the electric grid are scale-free networks. The authors demonstrated that ***scale-free networks can sustain large random errors with little performance degradation; however, deliberate attacks on key nodes can rapidly destroy the network***. The key nodes are simply the highly-connected nodes. The authors modeled a 10,000- node network under two scenarios: (1) **Failure** – random failure of nodes and (2) **Attack** – failure of key nodes. They tracked the performance of two critical network parameters: (1) (d) the network diameter or hops – the average length of the shortest paths between any two nodes and (2) C the cluster size distribution – C < 1 indicates the fragmentation of the network into islands. Increasing the diameter (number of hops) creates congestion and time delays and eventually disconnects portions of the Internet. *Figure 6* [5] demonstrates that the network is impervious to random failures up to 2.5% of the nodes, while attacks on key nodes increase the diameter from 4 to 17.

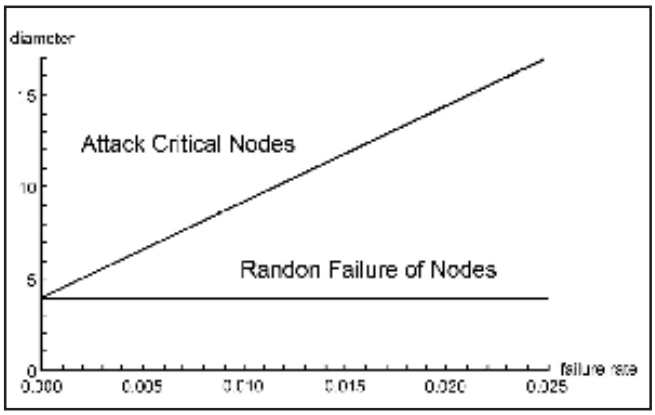


Figure 6: Network Diameter vs. Failure Rate [5]

Figure 7 illustrates the disintegration of the Internet under targeted attack (top half of diagram) and the robustness of the network to random failures (bottom half of diagram). The circles visually represent the distribution of cluster size. The figure shows the fragmentation of the Internet under failure rates of {5% - first column, 18% - second column, 45% - third column} for directed attacks {first row} and random failures (second row}.

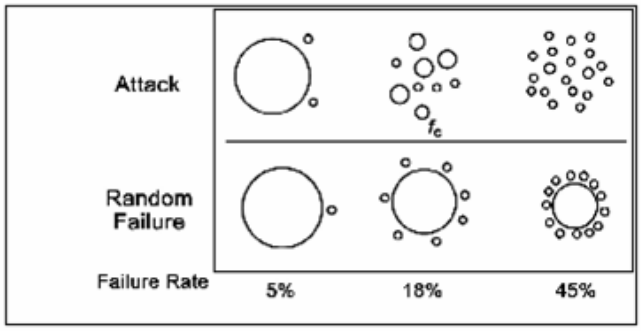


Figure 7: Cluster Size by Failure Rate [5]

At a critical frequency f_c (f=18%), an attack on 18% of the key nodes {first row, second column} causes the Internet to disintegrate into disconnected islands. Hence, under random failures on 45% of the nodes, 80% of the Internet remains connected while the rest dissolves into small clusters of sizes of 1 to 5 nodes {second row, third column}.

Critical infrastructure is robust under random failure, but extremely vulnerable to destruction under attack. Therefore; our Risk management approach must address this potential for catastrophic failure. Section 4 addresses actions to eradicate threats.

Alderson et al., in "Understanding Internet Topology: Principles, Models, and Validation" [10], describe effective and secure backbone design:

> Thus, the proposed first-principles approach suggests that a reasonably "good" design for an ISP network is one in which the core is constructed as a sparsely connected mesh of high-speed, low-connectivity routers which carry heavily aggregated traffic over high-bandwidth links. Accordingly, this mesh-like core is supported by a hierarchical tree-like structure at the edges whose purpose is to aggregate traffic through high connectivity. We refer to this design as *heuristically optimal topology (HOT)* to reflect its consistency with real design considerations.

Fortunately, the Internet backbone (Core) and connectivity to Independent Service Providers (Edges) has evolved to the topology described above. The primary causal factors shaping this topology are economic incentives and evolving router technology [11]. Lun Li, in a Cal Tech workshop, presents a picture of this topology, *Figure 8*, and validates its application to real networks [11]. Three other critical components of the Internet Autonomous Systems (AS), roughly corresponding to ISPs, connect to each other and the backbone through the Border Control Protocol (BGP).

Internet addresses are resolved through Domain Name Servers (DNS).

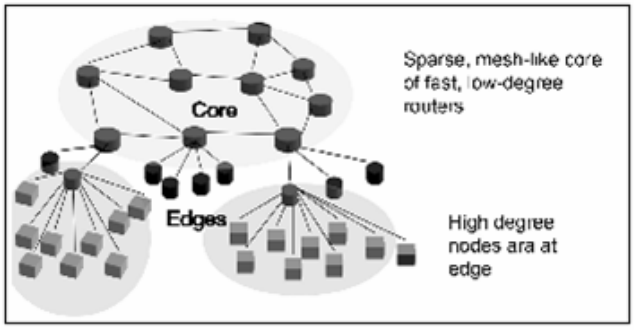


Figure 8: Backbone Topology [11]

Proposed Action 1: Structure Internet backbone impervious to attacks:

Intercede to alter the structure of the Internet backbone toward risk tolerance and eradicate threats that generate risk. Critical components of the backbone must be secured; these include the Domain Name Servers (DNS) and the Border Control Protocol (BCP).

Alderson, et al. [10] describes network engineering that hardens the Internet against attack.

THREAT ASSESSMENT

Threats exploit vulnerabilities in People, Processes, and Technology, exploding the myth of a technology solution. The complexity, rapid evolution, and widespread adaption of "universal" software create a steady stream of vulnerabilities.

The section develops the significant threats posed by: (1) phishing, (2) rootkits, and (3) botnets that exploit all three vulnerabilities. The section develops the causal link of threat, vulnerability, and impact of the Mariposa botnet. The fragility of infrastructure combined with the ***surprise-in-force*** capability of a botnet necessitates the actions, processes, and technology developed in the next section.

Phishing: A threat propagated through an e-mail, instant message, or social media. It depends on the intended victim's credulity in following instructions to open a dangerous payload. This payload exposes the computer to exploitation. Criminals use this breach to steal passwords, money from bank accounts, and information, and to propagate the threat. Phishing demonstrates that protecting against threats is not solely a technical problem. People trigger the Phishing threat through behavior.

Rootkits: Pose a serious threat to systems because they supplant critical functionality of the operating system by modifying the operating system kernel and critical system utilities. This creates a ***persistent threat***, the ability to operate for long periods of time undetected within a network. The attacker can execute unlimited exploits through a compromised operating system. Rootkits enable criminals to propagate viruses, worms, spyware, and adware. Command and control servers can then conscript these infected computers into a botnet. Faulty Processes or Technology permit root kits to compromise operating systems.

Botnets: *Figure 9* explains the operation of a botnet. After constructing or leasing a botnet (1 & 2), a criminal issues commands from a computer to Command and Control servers (1) which control an army of computers (2). The computers (4) are continually trying to infect and add new computers by broadcasting worms and malware (4) that exploit People and Technology vulnerabilities (5). The Command and Control servers provide a layer of protection and indirection between the Criminal, Command and Control servers (1), and the infected computers (4). The communication chain {1 → 2 → 4 → 6 → 7 or → 8} provides a mechanism for the criminal to continually update attack software in Company Victims (4, 5, 7). Scripts implanted in the Company Victims (7) exfiltrate passwords, credit card numbers, and information (8). The Company Host (7) is also impressed into the service of the botnet (7).

Botnets can launch denial of service attacks, spread malware and spam, and steal credit card information. Botnets typically use the IRC chat protocol for communication because it is widely available on target computers. The owners of infected machines are unaware of the infection unless they possess sophisticated detection methods. Faulty Processes or Technology permit the formation of botnets.

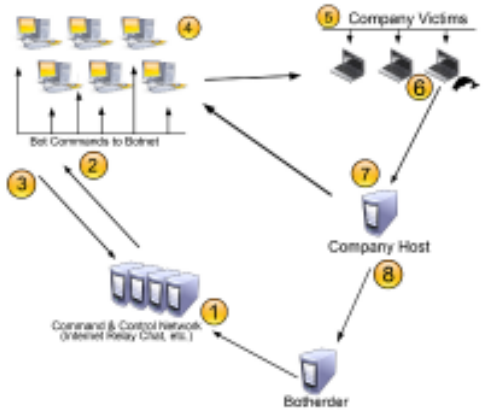


Figure 9: Botnet

I use Defence Intelligence's "Mariposa Botnet Analysis" [12] to relate the causal chain of threats/vulnerabilities/ impact for the Mariposa botnet. DefenceIntelligence first observed the Mariposa botnet in May 2009. Malware, distributed through Phishing, exploited People to establish the botnet. An .exe file was distributed in a form encouraging the receiver to open it, thereby infecting the computer. The computer then became a bot under the control of the Command & Control (C&C) servers. DefenceIntelligence identified and tracked 30 Mariposa C&C servers. The botnet possessed the capability to download and execute malware programs on command. This permits the criminal to infinitely extend the functionality of the malicious software. The criminal could also update the malware package on command, which reduces or eliminates the probability of detection from most detection mechanisms. The botnet stole credit card and bank account information, spread viruses, and launched denial of service attacks.

The complexity, rapid evolution, and widespread adaption of "universal" software (Microsoft Windows OS, Internet Explorer, Adobe Acrobat, and Word) create a steady stream of vulnerabilities. A relatively minor investment in discovering exploits by a criminal yields an enormous spectrum of targets. The openness of the Internet, protocols not designed for security, and operating system weaknesses create a rich field to propagate threats with impunity.

The paper "Modeling the Security Ecosystem – The Dynamics of (In)Security" [13] quantifies vulnerabilities. The paper analyzes vulnerability disclosures from 1996 to 2007. Three of the key findings are: (1) Over the last 10 years the number of vulnerabilities has grown at an increasing rate; (2) Compounding this, high-risk vulnerabilities constitute a higher percentage of the total; (3) Most exploits (78%) occur before public disclosure of the vulnerability (zero-day exploits). Zero-day exploits are attacks launched on vulnerabilities that have not been disclosed. These factors indicate a large and increasing asymmetry between an attacker's ability to exploit systems and a defender's ability to defend.

Proposed Action 2: Cultivate Awareness

Train People on how Threats are propagated internally by people. People inadvertently propagate Threats.

Proposed Action 3: Monitor Internal Threats
Focus sufficient efforts on monitoring for Threats emanating from within. Once a threat is embedded in a system it becomes a ***persistent threat*** posing great risk.

MITIGATING RISKS

The fragility of infrastructure, increasing vulnerabilities, the ineffectiveness of defense, and *surprise-in-force* capability of threats require active measures. The section proposes active counterintelligence through *tracking-attribution* and *active-countering.*

DefenceIntelligence partnered with Panda Security and the Georgia Tech Information Security Center to shut down the Command and Control servers of the Mariposa Botnet in December 2009. At that time there were an estimated 12.7 million compromised personal, corporate, government, and university computer systems. The data recovered from the C&C servers included account information, usernames, passwords, banking credentials, and credit card data from victims in over 190 countries [12].

An FBI press release about the Mariposa Botnet [14] reveals that foreign authorities in cooperation with the FBI arrested the developer and operators of this botnet. In February, Spanish authorities arrested three suspected operators of the botnet. In July, Slovenian authorities arrested the developer of the botnet.

The capabilities exist for ***tracking-attribution*** and ***active-countering*** and are presently employed in the private sector. The following two actions are the principal recommendations of this paper. Therefore, the paper develops justifications, actions, processes, and technology implementing these actions.

Proposed Action 4: Pursue ***tracking-attribution*** on Threats.

Tracking permits the analysis and containment of threats while attribution leads to the possibility of law enforcement actions.

Persistent threats are continually reaching back to their command & control server. This provides a ***beacon to track the threat***. Tracking can quantify the magnitude of the threat through identifying Command & Control servers, deciphering other targets, and recovering exfiltrated data. Attribution is not a precondition for active-countering; however, it is beneficial in negotiating treaties and monitoring compliance.

Proposed Action 5: Execute ***active-countering*** against Threats.

Eliminating Threats is the only current solution to the growing asymmetry between an attacker's ability to exploit systems and a defender's ability to defend.

The article identifies three significant threats. Unfortunately, DHS' "A Roadmap for Cybersecurity Research" [15] classified these threats as "hard problems." The study characterizes near-, medium-, and long-term solutions to "hard problems." The defensive solutions to combat malware, botnets, and rootkits fall within the medium- and long-term (5+ years to develop a technical solution). The "Emerging Cyber Threats Report for 2009" [16] identifies mechanisms of attack and current difficulties in defending against these attacks. Several of these mechanisms permit the stealthy accumulation of force, thereby enabling a surprise-in-force attack (botnets). Millions of compromised computers, controlled by many Command & Control servers, are capable of launching a massive denial of service attack at precise targets. Unchecked, the Command & Control servers can harden the compromised servers using encryption and complex programs to preempt countermeasures. This creates an asymmetry between the ease of attack and the difficulty to defend.

The risk of catastrophic failure to infrastructure under attack, the ineffectiveness of defense, and the massing of large botnets capable of surprise-in-force attacks requires the immediate execution of active measures such as ***tracking-attribution*** and ***active-countering***. Quoting General George S. Patton, Jr.: "***Fixed fortifications are monuments to man's stupidity***."

EFFECTIVE CYBER POLICY

Policymakers use Game Theory to predict adversaries' responses to policy actions before and during a crisis. These insights help shape prospective actions toward desirable outcomes.

This section evaluates policy efficacy using game theoretic methods pioneered by John Nash, who won the Nobel Prize in Economics in 1994 for this work. The section realizes this approach through Thomas Schelling's [17][18] elegant adaption to strategic conflict and Cold War nuclear strategy, which won the Nobel Prize in Economics in 2005. These works are central to current economic and social theories of bargaining, auctions, signaling intentions, the causes of war, and deterrence, from the advanced information on the 2005 Nobel Prize in Economics [19]. The 1994 economics laureates John Harsanyi, John Nash, and Reinhard Selten added solution concepts and insights that substantially enhanced the usefulness and predictive power of non-cooperative game theory. The most central solution concept is that of a Nash equilibrium. **A strategy combination (one strategy for each player) constitutes a Nash equilibrium if each player's strategy is optimal against the other players' strategies**.

Thomas Schelling's book *The Strategy of Conflict* (1960) launched his vision of game theory as a unifying framework for the social sciences. While Nash's formulations allow elegant mathematical analyses by way of abstracting from many realistic bargaining tactics, Schelling examines the bargaining tactics a player can use to tilt the outcome in his or her favor – emphasizing in particular that it may be advantageous to worsen one's own options to elicit concessions from the opponent. It can be wise for a general to burn bridges behind his troops as a credible commitment toward the enemy not to retreat.

Such tactics work if the commitment is irreversible or can only be undone at great cost, while commitments that are cheap to reverse will not elicit large concessions. However, if both parties make irreversible and incompatible commitments, harmful disagreement may follow.

The name – Game Theory – underplays the power and widespread adoption of this approach. Firstly, a game is an abstraction of reality. It cannot capture all the relevant factors, there are external factors not captured by the game. The structure of a game includes; 1) a set of players, 2) actions available to each player, 3) payoff resulting from each action, 4) order of movement, and 5) information available to each player before an action. Players are rational, they are expected to maximize their respective payoffs. Nash established the concept of an equilibrium in 1950. Nash's mathematical definition is equivalent to: ***Each player selects their best move (highest payoff) given the best moves (highest payoffs) of each of the other players.*** A player's deviation from this strategy results in a lower payoff.

Over the succeeding 60 years, game theory has advanced, addressing: (1) the uncertainty a player has over other players' payoff functions; (2) strategies formulated on probabilities of future actions; (3) multiple step games; and (4) tacit knowledge and signaling. Schelling outlined actions increasing the efficacy of National Security Policies in the Nuclear Arms Race. His contributions to Game Theory include bargaining tactics, tacit understandings, signaling, and other exploitable external factors.

This section addresses two criticisms of Game Theory: the assumption of rational players, and the ability to capture real scenarios. "Rational" does not mean mirror-imaging our beliefs and values onto adversaries. In the case of North Korea, its payoff function does not consider the welfare of its people, but would include the importation of luxury goods for the ruling elite. The process of formulating the payoff functions of adversaries requires IC intelligence on threats, and an evaluation of the efficacy of previous policies. Intelligence is an input to a collaborative process.

The mathematics of Game Theory often identifies multiple equilibria (solutions) to a Game. This multiplicity of solutions inhibits Policy analysis. Schelling transformed Game Theory by introducing nuanced external factors to resolve multiple equilibrium.

The article develops a Game (Hawk/Dove) which examines the consequences of U.S. policies from the expected responses of adversaries. The IC provides a critical understanding of adversaries through Intelligence and current threat profiles. This understanding contributes to formulating a Game which examines the consequences of multiple potential policies before committing to a policy. A properly formulated game divulges the complex interactions of multiple adversaries and the secondary consequences of decisions.

It is a valuable practice to confront decision-makers with a crisis scenario. The scenario provides the participants a view of group dynamics, variability of factors, and velocity of decision-making during a crisis. This interaction provides an enhanced understanding of adversaries and possible countering actions. A Game can serve as a critical component of this process. Refining the Game, after the scenario, also captures the knowledge of the diverse set of players. It is more than a
Plan; the Game captures plausible actions and expected responses. Quoting Dwight D. Eisenhower:

> ***In preparing for battle I have always found that plans are useless, but planning is indispensable.***

This process also fulfills the two objectives of the IC outlined in the first paragraph of the article: provide "actionable intelligence" and "feedback to policymakers on the impact of policy decisions."

Roger Myerson captures the complexity of the process in the following quote [20]:

> In such questions of deterrence, where the best strategy for us depends on how others will react to it, our strategic plan should be based on careful analysis of the actions that our potential adversaries will choose. But when we seriously endeavor to understand the choices of our adversaries, we may realize that their best plan of action must be based on their analysis of how we are likely to react to them. So we cannot understand our decision problem or our adversaries' unless we analyze our decisions and theirs together as part of an inextricably connected whole. Game theory has been developed as a framework for analyzing such interconnected decision problems.

I present a scenario demonstrating the complex interrelation of U.S. Policy and actions of U.S. adversaries. The Game is limited to two players. The Game develops a strategy of deterrence consistent with the process outlined by Myerson. The Game is not modeling cyber warfare. Terminology for diplomacy is important. "Intrude" refers to adversaries stealing U.S. intellectual and secret information and probing critical infrastructure to prepare for a future attack. "Counter" refers to the U.S. pursuing the recommended policy of ***active-countering***. Deputy Secretary of Defense Lynn uses the term "active defense." The Game could address cyber warfare through quantifying the payoffs of such warfare and adding an additional row and column to the Game. This, however, is beyond the scope of this article.

Scenario: ***Current U.S. Policies Magnify and Perpetuate the Cyber Threat*** *(Figure 10)*

A simple Game capturing elements of the present U.S. cybersecurity policy is Hawk/Dove.

Possible U.S. actions are represented by the first column. Possible Adversary actions are represented by the first row. A cell contains the payoffs (U.S. – first number, Adversary – second number) for the simultaneously and independently selected actions.

The scenario models the world as a series of games executed over an extended period.

U.S. Defend when Adversary Intrude results in U.S. payoff of **-2** and Adversary payoff of **1**. The Nash equilibria are highlighted with stars (***).**

The cases are Evaluated using Mathematica Code developed by Valeriu Ungureanu. The reader can download and experiment with different parameters [21].

US / Adversary	Defend	Intrude
Defend	***** (1,1) *****	***** (-2,1) *****
Counter	***** (1,-2) *****	(-4,-4)

Figure 10: U.S. Cyber Policy (Initial Case)

Deputy Secretary of Defense Lynn, in "Defending a New Domain" in *Foreign Affairs* [22] states:

> Over the past ten years, the frequency and sophistication of intrusions into U.S. military networks have increased exponentially. Every day,

U.S. military and civilian networks are probed thousands of times and scanned millions of times.

Adversaries have acquired thousands of files from U.S. networks and from the networks of U.S. allies and industry partners, including weapons blueprints, operational plans, and surveillance data.

How have the U.S. and adversaries arrived at an equilibrium unfavorable to U.S. National Security interests (upper-right cell – US Defend/Adversary Intrude)? The Game has an equilibrium desired by both players (upper-left cell), and another equilibrium with the Adversary not Intruding (lower-left cell). Schelling would state that the U.S. Policy of ***defend-only*** creates a "focal point," shifting the equilibrium to the U.S. suffering ***Constant Intrusions*** (upper-right).

Figure 11: ***Responses to Policies and Actions*** considers more realistic payoffs and possible U.S. Policies. The three scenarios are: (2) **U.S. More to Lose**, the continued U.S. concentration on Defense, (3) **Defend Only**, and (4) **Credible Deterrence**.

Case 2 – U.S. More to Lose: Of course, the payoffs should not be symmetric. The U.S. has far more to lose from tolerating intrusions, while adversaries have far more to gain from stealing U.S. secrets and technology. Altering the payoffs by doubling the Adversary's gains and increasing U.S. losses by 50% [Case 2] eliminates the desired equilibrium (upper-left), while maintaining the other two equilibria.

Case 3 – Defend Only: Limiting U.S. losses from Intrusions, which reduces adversaries gains, is neither a deterrent nor effective because of the limitations of technology previously discussed. There remains an equilibrium for the Adversary to Intrude and the U.S. to Defend. However, the favorable equilibrium of peace, from the initial case, reappears (upper-left).

Now the recommended U.S. strategy of **Credible Deterrence – Case 4.**

Case 4 – Credible Deterrence: The U.S. must make a "credible commitment" to deterrence. This requires a ***Policy and Actions*** intolerant of intrusions on U.S. infrastructure. The "credible commitment" arises from U.S. increasing intolerance to intrusions. Greater values of C (which represents increasingly aggressive responses from the U.S. to intrusions) capture this attitude and eliminate the equilibrium with Adversaries intruding (upper-right). Values of C>3 capture this "credible commitment" in the Game. The U.S. does not tolerate Intrusions on U.S. infrastructure. The U.S. executes active measures against Intrusions reinforcing Deterrence. This shifts equilibrium away from attacks on U.S. infrastructure (upper-right) toward peace (upper left).

> Recommendation: ***Effective U.S. Cybersecurity Policy and Actions***
>
> The U.S. will not tolerate intrusions against U.S. infrastructure, intellectual property, and secrets. The U.S. will ***track and attribute*** threats. The U.S. will ***actively counter identified*** threats.

Initial Case

Case 1 US/ Adver	Intrude
Defend	*** 1,1 *** *** -2,1 ***
Counter	*** 1,-2 *** -4,-4

US More to Lose

Case 2 US/ Adver	Defend	Intrude
Defend	1,1	*** -3,2 ***
Counter	*** 1,-2 ***	-4,-4

Defend Only

Case 3 US/ Adver	Defend	Intrude
Defend	*** 1,1 ***	*** -1,1 ***
Counter	*** 1,-2 ***	-2,-4

Credible Deterrent

Case 4 US/ Adver	Defend	Intrude
Defend	*** 1,1 ***	-1-**C**,1
Counter	***1,-2 ***	-4,-4

Figure 11: Responses to Policies and Actions

The current asymmetric situation of constant Intrusions against U.S. infrastructure is not expected using Game Theory. Schelling would state that the U.S. Policy of defend-only creates a "focal point" selecting the most unfavorable equilibrium for U.S. National Security. A deeper analysis reveals "extensive solutions" to the Game signaling a "tipping point" where the U.S., with very high probability, resorts to action. Deputy Secretary Lynn's statements and private sector actions eradicating the Mariposa botnet indicate that the U.S. has reached the "tipping point."

Information Assurance views Security in terms of the assuring 1) Confidentiality, (2) Integrity and (3) Access. Clearly, Confidentiality has been seriously compromised. ***I believe when adversaries also breach Integrity or Access the U.S .will adopt the policies outlined in this article***.

The paper's recommended Policy and Actions can lead to a peaceful equilibrium, preserving U.S. National Security.

PROCESSES AND BENEFITS

"Actionable intelligence" requires timely collaboration across a network spanning the IC, DoD, DHS, and the private sector. This network must rapidly channel real-time intelligence on cyber threats.

Efficiency and effectiveness require limiting the IC and government actors pursuing the two active measures proposed: ***tracking-attribution*** and ***active-countering***. Privacy concerns require two actors, DHS and an element of the combined DoD/IC. Effective Law Enforcement also requires extensive collaboration and a limited set of actors. The following processes achieve these objectives.

Proposed Process 1: ***Limit the execution of active measures*** to one element of DoD/IC and DHS. Private parties are already pursuing active measures. Coordinating with private parties is an open issue.

Tracking-attribution requires response teams deployable to government and private sites. The teams' processes, actions, and technologies are secret.

Proposed Process 2: ***Develop a network of Threat reporting*** culminating in one of the two previous elements. This network must include the private sector.

The network must have a semi-permeable barrier. Intrusions and Threat Intelligence flow up the chain. Incentive for the flow is confirmation of Threats eliminated flowing down.

The benefits of the proposed actions and policies advanced in this paper include:

(1) Increasing National Security by eliminating threats,
(2) Eliminating surprise-in-force (blitzkrieg) capabilities of adversaries,
(3) Attributing criminal and intelligence intrusions,
(4) Increasing the efficacy of law enforcement efforts,
(5) Reducing monetary losses from criminals,
(6) Decoupling criminal, terrorist, and state intrusions, and
(7) Reducing funding to achieve similar levels of risk.

References

[1] Office of the Director of National Intelligence, *The National Intelligence Strategy*, August 2009, http://www.dni.gov/reports/2009_NIS.pdf (accessed September 5, 2010).

[2] The White House, *The Comprehensive National Cybersecurity Initiative*, March 2010, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed February 23, 2011).

[3] The White House, *Cyberspace Policy Review ("60 Day Cybersecurity Review")*, May 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed September 05, 2010).

[4] Barabasi, Albert-Laszlo, "The Architecture of Complexity," August 2007, IEEE *Control Systems Magazine*, http://iris.lib.neu.edu/physics_fac_pubs/106/ (accessed February 23, 2011).

[5] Albert, Reka, Hawoong Jeong, and Albert-Laszlo Barabasi, "Error and attack tolerance of complex networks," *Nature*, Volume 406, 27 July 2000, http://www.barabasilab.com/pubs/CCNR-LB_Publications/200007-27_Nature-ErrorAttack/200007-27_Nature-ErrorAttack.pdf (accessed September 5, 2010).

[6] Albert, Reka, and Albert-Laszlo Barabasi. "Statistical mechanics of complex networks," *Reviews of Modern Physics*, Volume 74, No. 1, January 2002, http://www.barabasilab.com/pubs/CCNR-LB_Publications/200201-30_RevModernPhys-StatisticalMech/200201-30_RevModernPhys-StatisticalMech.pdf (accessed September 5, 2010).

[7] Yan, Guanhua, Stephan Eidenbenz, Sunil Thulasidasan, Pallab Datta, and Venkatesh Ramaswamy, "Criticality analysis of Internet infrastructure," *Computer Networks* 54 (2010), 1169-1182, http://www.sis.pitt.edu/~dtipper/3350/April_Paper4.pdf (accessed February 26, 2011).

[8] Kay, John, "Don't blame luck when your models misfire," *Financial Times*, March 2, 2011.

[9] Carreras, B. A., V. E. Lynch, D. E. Newman, and I. Dobson, "Blackout Mitigation Assessment in Power Transmission Systems," Hawaii Int. Conference on System Science, January 2003, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.153.7941 (accessed September 8, 2010).

[10] Alderson, David, Lun Li, Walter Willinger, and John C. Doyle, "Understanding Internet Topology: Principles, Models, and Validation,", IEEE/ACM Transactions on Networking, Vol. 13, NO. 6, December 2005, http://nsl.cs.sfu.ca/papers/ALWD05.pdf (accessed March 22, 2011).

[11] Li, Lun, John C. Doyle, Steven H. Low, David Alderson, and Walter Willinger, "Topologies of Complex Networks Functions vs. Structures," Caltech Wordshop, http://www.imss.caltech.edu/ (accessed March 26, 2011).

[12] DefenceIntelligence, "Mariposa Botnet Analysis, October 2009, http://defintel.com/docs/Mariposa_Analysis.pdf (accessed September 8, 2010).

[13] Frei, Stefan, Dominik Schatzmann, Bernhard Plattner, and Brian Trammell, "Modeling the Security Ecosystem – The Dynamics of (In)Security," http://www.techzoom.net/publications/security-

ecosystem/index.en (accessed September 8, 2010).
[14] Federal Bureau of Investigation, *FBI, Slovenian and Spanish Police Arrest Mariposa Botnet Creator, Operators*, July 28, 2010, http://www.fbi.gov/pressrel/pressrel10/mariposa072810.htm *(accessed September 8, 2010).*
[15] *Department of Homeland Security, A Roadmap for Cybersecurity Research, November 2009,* http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf *(accessed September 8, 2010).*
[16] *Georgia Tech Information Security Center, Emerging Cyber Threats Report for 2009, October 2008,* http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf *(accessed September 8, 2010).*
[17] Schelling, Thomas, *The Strategy of Conflict*, Cambridge,Massachusetts, Harvard University Press, 1960.
[18] Schelling, Thomas, *Arms and Influence*, New Haven, Connecticut, Yale University Press, 1966.
[19] The Royal Swedish Academy of Sciences, *Robert Aumann's and Thomas Schelling's Contributions to Game Theory: Analysis of Conflict and Cooperation*, October 10, 2005, http://nobelprize.org/nobel_prizes/economics/laureates/2005/ecoadv05.pdf *(accessed September 11, 2010).*
[20] Myerson, Roger B., "Force and Restraint in Strategic Deterrence: A Game-Theorists Perspective," http://home.uchicago.edu/~rmyerson/research/restrain.pdf *(accessed September 11, 2010).*
[21] Valeriu Ungureanu, "Set of Nash Equilibria in 2x2 Mixed Extended Games," http://demonstrations.wolfram.com/SetOfNashEquilibriaIn2x2MixedExtendedGames/ *(accessed September 11, 2010).*
All Demonstrations run freely on any standard Windows, Mac, or Linux computer. In fact, you do not even need *Mathematica*. You can interact with any demonstration using the free Wolfram CDF Player—for most platforms this happens right in your web browser. If you have *Mathematica* you can also experiment and modify the code yourself.
[22] William Lynn, "Defending a New Domain," *Foreign Affairs*, September/October 2010. Roger Myerson, *Game Theory: Analysis of Conflict*, Cambridge, Massachusetts, Harvard University Press, 1991, 91-108.

John G. Schwitz is a member of the Intelligence Community working on cybersecurity—securing critical infrastructure, information, and software. His work "Risk Evaluation of the Electric Grid" provides a foundation for risk assessments within the Community. He has more than 30 years experience in program management, software architecture, security, and risk management. His background in theoretical physics and finance has enabled his work in such domains as complex financial derivatives, risk analytics, and complexity of markets and security assessments. Previously, John served as an Enterprise Architect and Risk Manager at Unisys Corporation. He directed the development and review of all federal projects valued over $30 million for the Board of Directors and President. As Vice President of Technology at Sapient in New York, he consulted on major financial engagements with Goldman Sachs, J.P. Morgan, Royal Bank of Scotland, and New York Life. The projects ranged from foreign currency and risk management to transforming business segments to the Internet. During his career, John has engaged in numerous entrepreneurial ventures employing marketing, finance, and technology. He is a board member of the Professional Risk Managers International Association active in certification, recruitment, and training. He attended the Complete Course in Risk at George Washington University in 2008 and subsequently obtained the Professional Risk Management certification. John may be contacted at john.schwitz@prmcert.com or through his website, www.federalist.mobi.

Espionage and the Law of War

by Neil J. Beck

What enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge.

- Sun Tzu, *The Art of War*[1]

Two stories in the *New York Times* remind us of the importance and ambiguities—legal as well as moral—of intelligence operations. The newspaper on 24 May 2010 reported that General David Petraeus, the top American commander in the Middle East, authorized in September 2009 sending U.S. Special Forces into friendly and hostile nations in the Middle East, Central Asia, and the Horn of Africa to gather intelligence and build ties with local forces.[1] U.S. officials said the order also permits reconnaissance that could pave the way for military strikes should tensions with Iran escalate. According to the article, some in the U.S. military worry the U.S. soldiers, if captured, could be treated as spies and denied Geneva Convention protections offered to military detainees.[2] A separate story on 27 May 2010 detailed efforts by top lawyers at the State Department and the Pentagon to distinguish drone operators from unlawful combatants who can be prosecuted for violating the laws of war.[3]

Both articles reference how the corpus of the law of war—also called international humanitarian law (IHL)[4]—and customary international law (CIL) treat belligerents[5] captured while conducting intelligence operations, such as espionage, signals and imagery intelligence, and covert action.[6] The law of war and CIL do not prohibit belligerent states from such activities, but they mandate few protections for individuals caught by the enemy during a clandestine act and not wearing a uniform. Unlike soldiers captured in uniform, these individuals have no right to prisoner-of-war status. The legal foundation for this treatment is the principle of distinction, perhaps the bedrock of IHL. This treatment under IHL and CIL seems defensible as applied to belligerents that covertly use lethal force—the subjects of the second *New York Times* article—but it is less defensible when it is applied to belligerents who commit espionage—the subjects of the first article.[7]

Yet espionage—the gathering of information of military value in territories held by an adverse party using false pretenses or in a deliberately clandestine manner[8]—in war has largely escaped the attention of jurists, who appear more focused on covert action in peacetime. Perhaps this is not surprising. Covert action—which includes sabotage, paramilitary and psychological operations, black propaganda, and arms shipments—is controversial and dramatic. It can be physically coercive and blur the distinction between peace and war;[9] it also tends to be riskier and entails more serious legal and moral considerations than does espionage. A decision to undertake covert action ranks among the most serious displays of sovereign power.

This relative lack of attention would be sensible if espionage were unimportant to waging war or if IHL's treatment of espionage were analytically justified and consistent with its broader aims. Neither is the case.[10] This article suggests that jurists should reconsider how the law of war treats espionage. After tracing the development of IHL's treatment of war spies, it will argue that the principal justifications for denying prisoner-of-war status to them are unfounded, and that the current rules and norms undermine broader goals of IHL.

I. SPIES AND THE LAW OF WAR

Although spying in war is not illegal under IHL or CIL and does not create grounds for complaint between states under international law,[11] IHL offers little legal protection to war spies caught in the act. Persons engaging in espionage must wear the uniform of their armed forces to avoid treatment as a spy.[12] War spies caught in civilian clothing or an enemy uniform[13] have no legal right to prisoner-of-war status, unlike soldiers in uniform.

The legal status of war spies has emerged gradually from the conduct of belligerents over centuries and from successive rules of international law.[14] Even before state custom was prescribed in treaties, belligerents punished captured spies severely. During the American Revolution, American spy Captain Nathan Hale and British spy Major

John Andre were both executed after they were captured out-of-uniform, behind enemy lines, and with secret documents hidden in their clothing. General Howe denied Hale a formal court-martial and ordered his hanging the day of his capture.[15] Andre, an Adjunct General in charge of British Secret Intelligence, was tried and sentenced to death after some deliberation by the American Court of Inquiry, a board of fourteen general officers convened by General Washington.[16] The board found that he was a spy for moving behind enemy lines, out of uniform.[17]

The early regulation of espionage under IHL reflected the ruling of the American Court of Inquiry, identifying secrecy as the distinguishing criterion of espionage. The Instructions for the Government of Armies of the United States in the Field (the "Lieber Code"), promulgated during the U.S. Civil War, defined a spy as "a person who secretly, in disguise or under false pretense, seeks information with the intention of communicating it to the enemy."[18] This definition was affirmed by Article 19 of the 1874 Brussels Declaration on the Laws and Customs of War and by Article 24 of the Oxford Manual of the Laws of War on Land, which also tried to define who could *not* be considered a spy, namely those acting "without disguise."[19]

The 1899 Hague Convention codified these positive and negative definitions of "war spy" in a dual rule that distinguished "a spy acting clandestinely or on false pretenses" from "soldiers not in disguise."[20] The 1907 Hague Convention reaffirmed the rule in Article 29 of the annexed Regulations Respecting the Laws and Customs of War on Land and gave three requirements for an enemy to identify an individual as a spy:[21]

> A person can only be considered a spy when, [1] acting clandestinely or on false pretenses, [2] he obtains or endeavors to obtain information in the zone of operations of a belligerent, [3] with the intention of communicating it to the hostile party. Thus, *soldiers not wearing a disguise* who have penetrated into the zone of operations of the hostile army, for the purpose of obtaining information, *are not considered spies*. Similarly, the following are not considered spies: [s]oldiers and civilians, carrying out their mission openly, [e]ntrusted with the delivery of despatches intended either for their own army or for the enemy's army.[22]

Not wearing a uniform while gathering intelligence does not *necessarily* render an individual a spy, however, but it places the burden of proof upon the suspect.[23]

The Hague Convention Regulations do provide some minimal protections for war spies, but they fall far short of granting prisoner-of-war status. Article 30 of the Regulations states that a captured spy cannot be punished without previous trial, a minimal protection since the Convention does not define "trial" or stipulate procedural or substantive requirements. Article 31 contains a curious protection: if the enemy captures a spy after he has rejoined his army, he is to be treated as a prisoner-of-war, not a spy. The use of "rejoins" implies an anachronistic view that war spies withdraw their membership in their state's armed forces while they commit espionage, even though they are following orders of the government or military that employs them. A commentary shortly following the 1907 Hague Convention explains this view:

> [t]he spy is usually a soldier who has abandoned the recognized badge of his craft and his nation and adopted some disguise to shield his real character and intent. He has thrown away the insignia of his status, the evidence of his brotherhood among fighting men, and that for a purpose which the enemy has the greatest interest . . . to frustrate.[24]

According to one commentary, once a spy completes his act of espionage and returns to his forces, harsh punishment (if the enemy subsequently catches the spy) is unjustified because it can no longer deter the activity.[25] This explanation is unconvincing, however, because harsh punishment could send a message that, once a person commits espionage, he is forever a target for retribution. The protection in Article 31 might also reflect practical evidentiary concerns in the fog of war; if a war spy is captured after he returns to his military unit, evidence of his guilt probably is weaker than if he is caught in *flagrante delicto*. However, weak evidence might still be sufficient to convict him in politically-charged trials fueled by vengeance and a sense of victor's justice. The law of war gives protection to combatants based on their identity and activities at the time of their capture, when those factors can be easily and fairly determined.[26]

After the Second World War, many states sought to strengthen protections for belligerents from espionage.[27] At the 1949 Geneva Conference for the Protection of War Victims, the committee debate focused on concerns, including those of the United States and Britain, that The Hague Convention inadequately distinguished between spies and other civilians, imperiling belligerents' ability to wage war. The Commentary to Draft Article 3/A stated: "[e]nemy secret agents penetrate into the inner workings of the war machine, either to spy or to damage its mechanism. Many [d]elegations . . . fear that, under cover of the protection offered by the Convention, spies may be able to abuse the rights it provides for them."[28] The 1949 Geneva Convention Relative to the Protection of Civilian Persons in Time of War adopted the committee's proposal to curtail the ability of captured spies to communicate: "Where in

occupied territory an individual protected person is detained as a spy . . . , such person shall . . . be regarded as having forfeited rights of communication."[29] Article 68(2) of the Convention did provide another—albeit limited—protection for captured war spies: belligerents may execute spies in occupied territory if such punishment was legal in the territory prior to occupation.

Subsequent efforts to clarify the definition and treatment of war spies under IHL distinguished military reconnaissance activities and further limited legal protections for captured spies. The International Committee of the Red Cross (ICRC) in 1973 adopted a revised Draft Protocol on International Armed Conflict, in which the commentary to Article 40 clarified the difference between espionage and reconnaissance: "[w]hat distinguishes espionage from the legitimate quest for military information is its clandestine nature. The quest for military information is, it is true, always concealed . . . from the enemy; [but] the standing of [reconnaissance parties] should be unmistakably recognizable from their uniforms." That distinction was codified in the 1977 Geneva Convention Protocol for the Protection of Victims of International Armed Conflicts. Article 46(2) states, "A member of the armed forces of a Party to the conflict who . . . gathers or attempts to gather information shall not be considered [a war spy] if, while so acting, he is in the uniform of his armed forces." The first paragraph of Article 46 also explicitly denies prisoner-of-war status to spies captured while committing espionage.

Individuals captured while clandestinely gathering information with the purpose of communicating it to the enemy cannot claim prisoner-of-war status under IHL...

In sum, the current definition of "spy" closely follows the definition provided in the 1863 Lieber Code: "a person who secretly, in disguise or under false pretense, seeks information with the intention of communicating it to the enemy."[30] Individuals captured while clandestinely gathering information with the purpose of communicating it to the enemy cannot claim prisoner-of-war status under IHL, unlike individuals secretly gathering information while in the uniform of their armed forces. Captured spies lose the right to communicate and, if execution was permitted in the territory of the belligerent prior to the outbreak of armed conflict—they can be executed as long as the belligerent first affords them a trial.

The definition of "spy" and the rule that war spies are not entitled to prisoner-of-war status are also long-standing norms of CIL.[31] The Hague Regulations were signed without reservation in 1910, and Article 46 of Additional Protocol I of the Geneva Convention was adopted by consensus. Moreover, a review of national practice by the ICRC[32] found no official practice contrary to conventional IHL; the ICRC's survey of military manuals and national legislation showed that many countries, including Argentina, Britain, Ecuador, France, Germany, and the United States, follow Article 29 of the Hague Convention in defining "spies." A second survey of how states define the status of spies in their military manuals and legal codes revealed that spies uniformly are not entitled to prisoner-of-war status and may be tried and punished if captured in the act. For example, Canada's Law of Armed Conflict (LOAC) Manual states, "members of the armed forces engaging in hostilities while not in uniform may be treated as spies and lose their entitlement to [prisoner-of-war] status . . . they may be punished for [engaging in hostilities] but only after a fair trial."[33] In short, states consistently provide for the maximum level of deterrence allowed under international law and their criminal codes.

Although IHL leaves captured spies vulnerable to criminal punishment, it permits states at war to commit espionage. The Hague Regulations of 1907 draw this distinction. Article 24 of the annexed regulations to 1907 Hague Convention explicitly states that "[r]uses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible."[34] As Article 24 does not provide any exceptions, it does not appear to prohibit states from committing espionage in war,[35] and it suggests that an enemy belligerent has sole responsibility to deter spying against it.[36] Article 37(2) of Additional Protocol I reaffirms the acceptability of ruses of war. It defines ruses as "acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of [the law of war];"[37] espionage appears to qualify as a ruse of war. During armed conflict, then, spies are subject to punishment if captured but do not create legal responsibility for their state.[38]

The law of war does ban perfidy, but espionage does not qualify for the prohibition. Article 37 of Additional Protocol I to the Geneva Convention prohibits combatants from feigning civilian, non-combatant, or protected status by the use of UN or other neutral-party signs and emblems, but only when such acts: (a) "invit[e] the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence," and (b) result in the adversary's death, injury, or capture.

Indeed, CIL accepts that espionage is a fundamental tool of war. The Preparatory Document on Rules of Behavior of

Combatants, submitted by the ICRC in 1971 to the Geneva Conference of Government Experts on IHL in Armed Conflicts, states in Article 8 that "acts of espionage are legitimate acts of war."[39] Several military manuals reflect this view. Belgium's Law of War Manual states, "spying is not contrary to the law of war, and, as a result, does not constitute a war crime. Most countries provide, however, that spying is a crime [under domestic law] in order to protect their national interests and the interests of their armed forces."[40] The U.S. Naval Handbook and Ecuador's Naval Manual both state that "[s]pying during armed conflict is not a violation of international law. Captured spies are not, however, entitled to prisoner-of-war status."[41] Nigeria's Manual on the Law of War perhaps best exemplifies state custom:

> [f]or the purpose of waging war it is necessary to obtain information about the enemy. To get such information, it is lawful to employ spies and use soldiers and civilians of the enemy for committing acts of treason. But although this practice by the state is considered legitimate, lawful punishment under the municipal law may be imposed upon individuals engaged in espionage or treason when they are caught by the enemy.[42]

II. JUSTIFICATIONS AND SHORTCOMINGS OF LIMITED PROTECTION

Denying prisoner-of-war protection to captured war spies has three principal justifications. First, spies are morally unworthy of the protection offered to soldiers in uniform. Second, IHL's regulation of espionage is consistent with the notion that combatants should be protected to the extent that they distinguish themselves from non-combatants, a fundamental goal of the law of war.[43] Third, rewarding spies with protection would incentivize espionage during armed conflict, which could expand its scope and extend its duration. However, closer scrutiny raises doubts about the strength of these justifications. In addition, offering minimal protection to captured war spies undermines the corpus of the law of war in three distinct ways. First, by treating states and spies inconsistently, IHL undermines its goal of discouraging espionage. Second, IHL misses an opportunity to strengthen "effective compliance" with its fundamental principles. Finally, IHL's failure to distinguish spies caught gathering secrets from saboteurs, assassins, and paramilitary forces treats unlike activities equally.

The first justification for minimal protection is that war spies are morally unworthy of the protection offered to military personnel in uniform. Sneaking behind enemy lines disguised as a civilian, sheltered from the dangers of combat, is unbecoming of a professional soldier. Opponents of granting prisoner-of-war status to spies can point to philosophy and history to buttress their case that espionage is underhanded and immoral. In *Fair Play*, former chief of CIA counterintelligence James Olson concisely lays out several of these arguments.[44] He points to the Old Testament book of Deuteronomy—"Always be fair and just, so that you will occupy the land that the Lord your God is giving you and so that you will continue to live there"—and that New Testament book of Matthew—"Therefore all that you wish men would do to you, so also you do to them"—to argue that some Biblical passages do not allow for any notion of the "greater good" to justify a dishonest act.[45] Olson also surmises that Aristotle would find modern espionage "hateful and mean." Justice to Aristotle is universal, not situational. According to his theory of the mean, every virtue exists along a continuum between extremes of opposing vices, and the mean is determined by what would promote a virtuous result; as Olson explains, this does not license moral relativism.[46] Olson also argues that the deception and manipulation that is vital to espionage appears to violate German philosopher Immanuel Kant's Categorical Imperative, particularly the so-called Humanity formulation: "Act in such a way that you always treat humanity, whether in your own person or in the person of any other, never simply as a means, but always at the same time as an end."[47] Indeed, Kant in *The Science of Right I* singles out spying for approbation:

> Among these forbidden means are to be reckoned the appointment of subjects to act as spies, or engaging subjects or even strangers to act as assassins, or poisoners, or even employing agents to spread false news. In a word, it is forbidden to use such malignant and perfidious means as would destroy the confidence which would be required to establish a lasting peace thereafter.[48]

Opponents of greater protection for war spies can also find support in the statements of jurists and statesmen. William Edward Hall, in his *Treatise on International Law* in 1909, wrote, "[it] is legitimate to employ spies; but to be a spy is regarded as dishonourable, the methods of obtaining information which are used being often such that an honourable man cannot employ them."[49] Henry Stimson, U.S. Secretary of State under President Hoover, agreed with these sentiments at the acme of post-World War I pacifism. In 1929 he closed MI-8, the State Department's cryptanalytic office, famously saying, "Gentlemen do not read each other's mail."[50]

However, proponents of greater protection for spies under the law of war can also point to philosophy and history for support. The story of the prostitute Rahab in the Old

Testament book of Joshua, as Olson relays it, suggests spying is not intrinsically immoral in Judeo-Christian thought.[51] Rahab protected two spies of Joshua from the King of Jericho's men, an act for which she is praised in both the Old and New Testaments. Olson also convincingly argues that Saint Thomas Aquinas' articulation of what is known as the "just war" doctrine can equally apply to espionage, and he hints that espionage can help to make a war more just.[52] Moreover, utilitarianists such as Jeremy Bentham—"[Security] is the foundation of life, of subsistence, of abundance, of happiness; everything depends on it"—and John Stuart Mill—"the sole end for which mankind is warranted . . . in interfering with the liberty of action of any of their number, is self-protection"—could support espionage undertaken for self-defense and security.[53]

Even the historical events discussed earlier are more nuanced. At the hanging of British spy John Andre, many American officers, including General Washington, admired Andre's gallantry and mourned his death. Washington would have traded him for Benedict Arnold, but after the British refused Washington felt any sign of mercy would encourage more British spies.[54] U.S. Secretary of State Stimson's own moral qualms with espionage evaporated as the winds of war rustled in the 1930s. He became an outspoken proponent of confronting Japan's aggression across East Asia, and by 1940—when President Roosevelt appointed him Secretary of War—he had reversed his opposition to intelligence activities.[55]

Proponents of greater protection might also argue that espionage in wartime, being necessary for the public good, is morally just. Prior to accepting his first and last spying mission, Nathan Hale agonized over the decision before stating to a friend, "Any kind of service necessary to the public good becomes honorable by being necessary."[56] Hale perhaps could have turned to Cicero for reassurance. Cicero famously wrote, "In time of war, the laws fall silent," but this single quote does not capture his thinking on necessity and morality. As Olson recounts, Cicero wrote that "[e]xpedience sometimes clashes with honesty," and in that circumstance, the right action is to do what better serves society or the state.[57]

It is difficult to argue that espionage is not a necessity in war. American military author Colonel A.L. Wagner wrote, "[s]pies are indispensably necessary to a general; and other things being equal, that commander will be victorious who has the better service."[58] During the Revolutionary War, General Washington spent ten percent of his military apportionment on intelligence activities, having learned the importance of spies as a young officer in the French and Indian War, when he led his troops into a French ambush after his British commander refused to collect intelligence on nearby enemy forces. The episode led Washington to write, "[t]here is nothing more necessary than good intelligence to frustrate a designing enemy and nothing that requires greater pains to obtain."[59] He became a skilled spymaster. In 1776, as the American cause flickered during a string of humiliating defeats, Washington personally recruited John Honeyman, an Irish immigrant and weaver, to report on enemy capabilities at Trenton. Washington asked Honeyman to move to central New Jersey, enter the cattle business, and supply meat to nearby British forces. He also arranged for Honeyman to be publicly denounced as a British sympathizer. His cover established, Honeyman developed close relationships with British officers in Trenton. On 22 December, Washington had Honeyman "arrested," creating an opportunity to debrief him without signaling he was a spy. Honeyman provided a map showing all enemy locations in Trenton and reported that the Hessians had not built fortifications, thinking the Americans were hunkered down in Valley Forge. Washington's subsequent attack on Trenton scored an important political victory that refortified sagging American morale.[60]

The role of technology in combat has not diminished the importance of human spies.

The role of technology in combat has not diminished the importance of human spies. In February 2003, a month before the United States invaded Iraq, a German intelligence officer in Qatar gave to U.S. Defense Intelligence Agency officials a copy of Saddam Hussein's new Baghdad Defense Plan, a major revision of his decade-long strategy that American war planners were studying.[61] On 17 March, three days before the United States invaded Iraq, Germany evacuated its embassy in Baghdad, but at least two German intelligence officers remained in a Baghdad safe house. They helped U.S. forces identify "non-targets"—such as embassies, schools, and hospitals that should not be attacked—and, according to a German media source in the Pentagon, they helped select bombing targets. U.S. intelligence officials on 7 April asked their German counterparts to have their officers in Baghdad verify that a convoy of armored vehicles had parked at a restaurant frequented by Saddam Hussein. After receiving that confirmation, U.S. bombers leveled the restaurant with satellite-guided bombs.[62] Hussein escaped, but such pinpoint targeting may have increased the Iraqi generals' feeling of vulnerability and contributed to their decision to abandon organized resistance in the capital.

Moreover, deception in war often is revered. The ancient Chinese military strategist Sun Tzu wrote, "All warfare is based on deception. Hence, when able to attack, we must

seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."[63]

Many Americans are familiar with Operation FORTITUDE during World War II, in which U.S. and British forces engaged in elaborate ruses to convince Berlin that the invasion of Europe would occur not at Normandy, but at Pas de Calais and in Norway. It included fake radio traffic, poorly camouflaged dummy landing craft massing in English ports, fields of papier-mâché and rubber tanks, and fake oil docks, among other deceptions. Hitler, informed of the buildup by German reconnaissance planes and spies, cancelled the transfer of five army divisions from Norway to France just weeks before D-Day. Even during the landings at Normandy, Hitler was convinced they were a ruse and held back critical Panzer divisions and reinforcements for landings at Pas-de-Calais that never occurred. Paraphrasing Churchill, author Steven Ambrose wrote, "[N]ever in the history of warfare have so many been immobilized by so few."[64]

Choosing to honor the act but vilify the actor is to make an arbitrary distinction—a sworn enemy of law. Opponents of greater protection for war spies under IHL will need to look to other rationales.

In summary, the view that espionage is underhanded and immoral is not unfounded in philosophy and history, but it also is not unchallenged. In addition, viewing spies as dishonorable seems incongruent with the value placed on espionage and deception in war. Choosing to honor the act but vilify the actor is to make an arbitrary distinction—a sworn enemy of law. Opponents of greater protection for war spies under IHL will need to look to other rationales.

Second, opponents of greater protection for captured war spies may argue that the current treatment under IHL helps to uphold the fundamental principle of distinction in IHL. Article 48 of Additional Protocol I states that armed forces must always distinguish between combatants and military targets on the one hand and the civilian population and civilian objects on the other, a notion rooted in the "Just War" tradition. Article 48 obliges combatants to distinguish themselves by wearing a uniform, carrying a distinctive sign, or carrying their weapons openly. The law thus adopts a case-by-case, evidentiary approach rather than a bright line. Still, many armed forces hold fast to the traditional norm of wearing a uniform, albeit sometimes their military manuals present that requirement with qualifying adjectives.[65]

Opponents of greater protection for captured war spies might argue that such treatment is equitable in that, under the current rule, all captured combatants receive treatment in direct relation to their observable status as legitimate military targets. Military reconnaissance teams also try to gather intelligence behind enemy lines, but their uniforms or other distinguishing marks signal their legitimacy as targets and their acceptance of that status. The personal risk that uninformed soldiers endure in openly carrying out their duties reflects a sense of fair play in war and, if they are captured, that same fairness suggests they should receive prisoner-of-war status. War spies, opponents would say, also receive reciprocal treatment. Disguised as civilians or in the uniform of their enemy, spies knowingly signal that they are not legitimate targets. When captured, they are treated as any other criminal under domestic law; they have no claim to the protections granted to uniformed soldiers because they did not present themselves as such and accept the accompanying risk. Judge Abraham Sofaer, former Legal Advisor to the U.S. Department of State, captured this sentiment in remarks published in 1987:

> A fundamental premise of the Geneva Conventions has been that to earn the right to protection as military fighters, soldiers must distinguish themselves from civilians by wearing uniforms and carrying their weapons openly . . . Fighters, who attempt to take advantage of civilians by hiding among them in civilian dress, with their weapons out of view, lose their claim to be treated as soldiers. The law thus attempts to encourage fighters to avoid placing civilians in unconscionable jeopardy.[66]

Of course, many modern combatants do not effectively distinguish themselves from civilians, and recent evolutions in warfare present new challenges to the distinction principle. With precision long-range artillery, automatic weapons, and air power, many combatants are barely or not at all visible on the horizon—a major shift from earlier wars—and therefore have less operational need to distinguish themselves. Moreover, the proliferation of guerrilla fighters and insurgents in armed conflicts, often dressed in civilian clothing, means that a large subset of contemporary combatants do not physically distinguish themselves at all from civilians. Indeed, some combatants—particularly in conflicts marked by asymmetry in technology, training, and resources—choose not to distinguish themselves almost certainly to create some modicum of advantage, albeit unlawfully. Leaving this class of fighters aside, to the extent that combatants who only minimally distinguish themselves from civilians are able to claim prisoner-of-war status upon their capture, the

law of war may create a horizontal inequity. War spies—perhaps equally indistinguishable at a distance—are automatically denied such protection.

Regardless of what individual states and combatants do in practice, Additional Protocol I requires combatants to distinguish themselves from civilians. That some combatants do not follow this rule in practice is a violation of the rule, not evidence that the rule is flawed. Even so, denying prisoner-of-war protections to captured war spies for violating the principle of distinction seems to fall trap to an excessive sort of legalism—that is, rigid adherence to a rule even if compliance does not advance the objective of that rule. To be clear, the objective of the principle of distinction is to limit the scope of violence to lawful combatants and to protect civilians.[67] To endanger civilians, a belligerent would have to suspect that civilians actually are spies gathering intelligence and therefore are legitimate targets of military force. Perhaps, but the risk seems overstated, particularly if the spies are unarmed and only committing espionage, and are not participating in sabotage or other coercive covert action. The rational response to a suspected spy would seem to be a counterintelligence operation and an arrest, not a military attack.

A third justification for limited protection for captured war spies is that, because espionage can help neutralize an enemy's advantages and prolong war, IHL in discouraging espionage helps to limit the duration of combat. For example, a relatively weak state involved in a hypothetical war with Russia may use asymmetrical tactics to neutralize Russian conventional strength and "decelerate" the conflict."[68] Espionage, in theory, would tend to support that strategy. By clandestinely gathering information on Russian intent, technology, diplomatic maneuvers, and economic and political vulnerabilities, the adversary may be able to prolong a conflict, leading to greater destruction and loss of life. By protecting its "soft underbelly"—the economic, political, and institutional drivers of its ability to wage war—Russia may limit the scope and duration of the armed conflict. Assuming that domestic laws against espionage have some deterrent effect, limiting protections available to captured war spies under the law of war is worthwhile, even if law is never as effective as counterespionage in stopping spies.

This justification is nearly impossible to disprove, but it seems equally plausible that the reverse is true—that espionage may limit the scope and duration of a war. Given the lethality of modern warfare, an armed conflict can easily exact a humanitarian toll far in excess of the political, economic, and military advantages at stake, and global economic interdependence and information flows magnify the impact of war far beyond the battlefield. If espionage can improve the quality of information available to the warfighter, it can be a limiting factor on the scope of combat operations and the likelihood of miscalculation. Espionage can help a belligerent understand its enemy's true intentions, location, and political will to fight, which should help it anticipate and avoid dangerous escalations of force, accurately apply the minimum force necessary to achieve its objectives, waste fewer resources and lives attacking low-yield targets, and grasp opportunities to return to the negotiating table. If these theoretical assertions are true, and war spies can limit the number of wars, their scope, and their duration, any attempt by IHL to discourage spying—even on the margins—is counterproductive to its aims.[69]

The weaknesses of these justifications for limited protection for captured war spies are compounded by three additional theoretical shortcomings. First, the law of war's unequal treatment of spies and their states fails to discourage acts of espionage, and therefore does not protect belligerents or non-combatants from espionage, which presumably are intended goals of denying prisoner-of-war status to spies. As discussed earlier, under the law of war, captured spies who were ordered to commit espionage do not receive prisoner-of-war status and can be tried as common criminals. Yet states can commit espionage, which arguably is a ruse of war because it involves misrepresenting one's identity in order to persuade an adversary to recklessly disclose confidential information.

Consider the following hypothetical steps in an espionage operation: (1) State X, at war with State Y, identifies information gaps on State Y and decides to commit espionage; (2) an official in State X orders a member of that state's intelligence service or armed forces to spy in State Y; (3) the intelligence service of State X provides funding, communications, and other support to enable the spy to fulfill his mission; (4) the spy, following orders and using the resources provided by State X, spies on State Y. Under the law of war, only the fourth step creates responsibility, and that responsibility is borne by the spy alone, leaving him vulnerable to severe penalties. Meanwhile, State X bears no responsibility under international law for its role.

It is clear the law of war makes no real attempt to discourage states from spying.

Looking at the costs and benefits of espionage to states, then, it is clear the law of war makes no real attempt to discourage states from spying. The cost of espionage is no greater than the cost of an overt reconnaissance mission; whether the enemy captures a disguised agent or a

uniformed soldier, it removes him from serving as a tool of his state. However, from the state's perspective, the benefits of spying are likely to exceed the benefits of military reconnaissance, since a disguised agent presumably can access sources and information that uniformed soldiers cannot. The only constraint on the state is to convince individuals to accept the risk of capture, trial, and execution, which is probably a minimal hurdle during armed conflict.

That said, IHL has no effective way to raise the costs of espionage to a level sufficient to convince states to abandon spying during armed conflict. Therein lies the problem; ending asymmetrical responsibility by outlawing espionage in war—short of making espionage a war crime—would have little impact, if any, on the level of espionage. Only the state committing espionage—not the individual officials ordering such action—would be held responsible under international law, and the diplomatic costs attendant to state responsibility are simply insufficient to abandon spying as a tool of war.

Even if the preceding argument is incorrect, meaning the law of war's treatment of captured war spies has some deterrent effect on the incidence of espionage in war, that would only raise a new complaint. By deterring espionage, the current treatment of war spies would be a missed opportunity to increase "effective compliance" with principles of the law of war. "Effective compliance" has several definitions in academic literature,[70] and a plausible adaptation here is that effective compliance is the combination of a belligerent adhering to a procedural requirement of the law of war and the complying act achieving the intended result of the requirement. For example, compliance with the principle of distinction requires combatants to differentiate between military and civilian targets. "Effective compliance" means that a good faith effort to distinguish military and civilian targets leads to the intended consequence—protecting civilians from armed conflict.

The current treatment of war spies limits belligerents' "effective compliance" with the principle of distinction. Imagine a military target surrounded by structures whose uses cannot be identified from satellite reconnaissance, research, or overt observation. Without intelligence from spies on the ground, a belligerent might make the inaccurate—but potentially lawful—judgment that the surrounding buildings also have a military use and are viable targets. In that situation, human intelligence could enable combatants to accurately distinguish military from civilian targets and protect civilians from attack.

Similarly, the current treatment of war spies is a missed opportunity to increase effective compliance with the principle of proportionality. According to Additional Protocol I, the principle states that an attack is prohibited if it causes incidental loss of civilian life, injury to civilians, or damage to civilian objects that is excessive in relation to the anticipated concrete and direct military advantage of the attack.[71] Espionage promotes "effective compliance" with proportionality. Consider a belligerent determining whether to attack a military bunker, unaware that civilians are seeking refuge inside of or near it. If espionage could have uncovered their presence, it would increase the likelihood that, when the belligerent decides the direct military advantage is proportional to the expected collateral damage, he is in fact correct.

Finally, the treatment of war spies is flawed because IHL does not adequately distinguish between spies and saboteurs, assassins, and other covert actors whose activities raise more serious challenges for complying with the laws of war. In theory, covert actors have no incentive to spy only and not engage in physically coercive acts. Under Article 44 of Additional Protocol I, saboteurs and assassins fail to meet the requirements of lawful combatants, and, like war spies, they have no right to prisoner-of-war status. They can be tried for their acts as common criminals, albeit with the "fundamental guarantees" of Article 75 of Additional Protocol I for all such persons facing trial and sentencing for penal offenses related to the armed conflict. In other words, war spies are entitled under Article 75 only to the minimum protections guaranteed to saboteurs and assassins, whose activities are more coercive, destructive to life and property, and likely to endanger civilian populations and spread the use of deadly force beyond the battlefield. This lack of distinction under the law for fundamentally dissimilar activities does not help to discourage covert actors from more coercive acts, presumably a goal of IHL. If a covert actor will be punished equally for gathering information or sabotaging civilian infrastructure—a question of domestic law only made relevant by IHL's minimal protections for spies, he may be indifferent between the two and choose the act most likely to quickly impact the war effort.[72]

III. SUPPORT FOR THE STATUS QUO UNLIKELY TO CHANGE SOON

Despite the counterarguments to the justifications for denying prisoner-of-war status to war spies and the additional shortcomings that were discussed above, state actors almost certainly will reject reversing the rule, primarily because of the potential harm to the principle of distinction. For the first time, lawful combatants with a right to prisoner-of-war status would be completely indistinguishable from civilians. The distinction principle already is under pressure from the rise of insurgencies, guerrilla fighters, and criminal organizations that openly flout the law of war by purposefully trying to blend in with

civilians while engaged in hostile acts. Governments surely will want to strengthen, not weaken, the principle of distinction.[73]

Concern for the principle of distinction is not the only hurdle facing proponents of a rule change, however. A second challenge is that many states probably do not consider granting prisoner-of-war status to spies to be in their national interest. Western military powers, for example, may see their relatively open economies and societies as especially vulnerable to espionage during war and not wish to impose any constraint on their ability to deter espionage through harsh criminal punishments. States with relatively little military power and less capable intelligence services might not see any benefit from a rule change as likely. In addition, some states may have no interest in creating yet another class of enemy individuals they would need to protect if captured.

To address these concerns, advocates of a change in the rule will have to add muscle to the arguments discussed here, i.e., that granting prisoner-of-war status to captured war spies is unlikely to endanger civilians. Empirical studies of the impact of espionage on civilian casualties and on compliance with distinction and proportionality could make a valuable contribution to any debate, but much of the information probably is highly classified and may not be shared across governments. Proponents of change at least should propose a new rule that draws a clear line between spies gathering information and other covert actors conducting physically-coercive actions, such as sabotage; the latter would not receive any new protection under the law of war, and the former would be carefully defined. This effort almost certainly will be measured in years, not months, as it will require extensive collaboration, commentary, and revision with stakeholders in government, the military, academia, and non-profits.

This effort would be helped, albeit only on the margins, if the legal community were to consider it alongside other amendments to IHL provisions. An overhaul appears very unlikely in the near term, although two broader changes in the international order could, over time, expose a need for wide-ranging revisions to adapt the law of war to new realities on the ground. One is the possible erosion of the "unipolar moment" in international relations and its replacement by a relatively less stable multipolar era. The second change is that states' monopoly over the use of force—a hallmark of the international order since the 17th century—seems to be gradually eroding due to the rise of non-state actors capable of waging protracted, asymmetric wars. Of course, if that erosion reaches a critical mass, the treatment of captured war spies will be the least of IHL's worries.

Notes

[1] *Sun Tzu on the Art of War*. *Lionel Giles, Trans., May, 1994.* Accessed November 15, 2006, at <http://www.fas.org/man/artofwar.htm>.

[2] Mark Mazzetti, "US is Said to Expand Secret Actions in Mideast." *The New York Times*, 24 May 2010. Accessed at <http://www.nytimes.com/2010/05/25/world/25military.html?scp=3&sq=donald%20rumsfeld&st=cse>.

[3] The article assumes, perhaps incorrectly, that the Geneva Conventions—which assume that a state of armed conflict exists—apply in this circumstance.

[4] Charlie Savage, "UN Official to Ask US to End CIA Drone Strikes." *The New York Times*, 27 May 2010. Accessed at <http://www.nytimes.com/2010/05/28/world/asia/28drones.html?ref=global-home>.

[5] IHL is known traditionally as the law of war. This paper uses both terms interchangeably. Some observers find "international humanitarian law" to be a misleading moniker, since the body of international treaties, codes, and customs comprising IHL is distinct from human rights law and does not pass judgment on the legality of war. Instead, IHL regulates the conduct of hostilities and the protection of persons during an armed conflict.

[6] The term "belligerent" in IHL generally refers to a person, group, state, or other entity that is a lawful party to an armed conflict. For example, Article 1 of the 1907 Hague Convention states that persons "shall be regarded as belligerents if they carry arms openly and if they respect the laws and customs of war."

[7] This paper distinguishes between covert action—a category of intelligence operations—and covert acts, which include any act undertaken in a clandestine manner. For a thoughtful discussion on the types of intelligence operations, see James Olson, *Fair Play*, Potomac Books, 2006, pp. 239-240. See also Abram Shulsky and Gary Schmitt, *Silent Warfare: Understanding the World of Intelligence*, Brassey's Inc., 2002. For a critical analysis of the types of covert action, see Loch K. Johnson, "On Drawing a Bright Line for Covert Operations," *American Journal of International Law* 86 (1992), pp. 284-285.

[8] Thucydides, *History of the Peloponnesian War*. Rex Warner, trans., Penguin Books, Publisher, 1954, pp. 432, 438.

[9] Hilaire McCoubrey, *International Humanitarian Law: The Regulation of Armed Conflicts*, Gower Publishing Co., 1990, p. 86.

[10] The demarcation between peace and war is not as clear at the dawn of the 21st century as it was even a few decades ago. Given the simultaneous rise of non-state actors committed to destroying state adversaries and the relentless diffusion of technology related to weapons of mass destruction (WMD), it takes little imagination to identify plausible counter-examples. A common hypothetical is the United States undertakes covert paramilitary action inside a sovereign nation, which is at peace with the United States, to deny WMD materials to terrorists.

[11] Belligerents constantly require current intelligence on the intent, strategy, and capabilities of their enemies; in contrast, covert action during peacetime is a choice for dealing with a highly fact-dependent situation. For example, the U.S. decision to covertly train the Hmong to disrupt North Vietnamese supply routes inside Laos was made necessary—and possible—by the convergence of several factors: North Vietnamese violation of Laos territory, the withdrawal of all foreign military forces from Laos under the 1954 Geneva Accords, the warrior nature of the Hmong, and the ongoing struggle against communism in Laos.

For more discussion, see James Lilley, *China Hands: Nine Decades of Adventure, Espionage, and Diplomacy in Asia*, Public Affairs, 2004, p. 108.
[12] Hilaire McCoubrey, *International Humanitarian Law: The Regulation of Armed Conflicts*, Gower Publishing Co., 1990, p. 86.
[13] Hague Convention Regulations Respecting the Laws and Customs of War on Land, Art. 29, October 18, 1907, in Roberts and Guelff, *Documents on the Laws of War*, Oxford University Press, 2004, p. 78.
[14] A spy might use a variety of disguises—including enemy or neutral military uniforms—to conceal his actual identity or even to induce the enemy to trust him.
[15] John Kish, *International Law and Espionage*, Martinus Nijhoff Publishers, 1995, p. 144.
[16] "Captain Nathan Hale," website of the Connecticut Society of the Sons of the American Revolution, <http://www.ctssar.org/patriots/nathan_hale.htm>.
[17] J.M. Spaight, *War Rights on Land*, London, 1911, p. 210.
[18] "The Death of John Andre," Spy Letters of the American Revolution Collection, Clements Library, University of Michigan, <http://www.si.umich.edu/spies/stories-arnold-4.html>.
[19] "Instructions for the Government of Armies of the United States in the Field," Article 88, 1863.
[20] Kish, 145. The Oxford Manual of the Laws of War on Land and the 1899 and 1907 Hague Conventions do not define "disguise." The term deserves a broad definition given its potential manifestations. A reasonable definition of "disguise" in the context of espionage is "any attempt by an individual to obfuscate his identity as an enemy combatant seeking to clandestinely gather information and communicate it to the enemy." This definition would properly exclude from classification as spies the U.S. Special Forces teams which secretly slipped into Taliban strongholds to identify viable military targets but did not conceal their identity as U.S. soldiers. The definition would properly not exclude from classification as spies any uniformed soldier sent to negotiate with an enemy commander under a flag of truce who also intends to gather intelligence on enemy formations or readiness.
[21] Kish, 145.
[22] Kish, 145.
[23] Hague Convention Regulations Respecting the Laws and Customs of War on Land, Art. 29, October 18, 1907 (emphasis added).
[24] McCoubrey, 86.
[25] Spaight, 203.
[26] Maj. Richard Baxter, "So-Called 'Unprivileged Belligerency': Spies, Guerrillas, and Saboteurs," p. 331.
[27] There are obvious limits to the "fog of war" explanation. Lawful combatants can be charged with war crimes long after capture. The evidentiary concerns that protect ex-spies stem from the difficulty of establishing identity when little physical evidence exists and the suspect was disguised. War crimes, on the other hand, often produce large amounts of physical evidence—dead bodies, razed villages, etc.—and the perpetrators may not have been in disguise.
[28] The motivation to protect against espionage does not appear to have stemmed from any one incident. Perhaps because the stakes during the global conflict were so high—many parties were fighting for their very survival as independent states—the victors simply wanted to strengthen their ability to wage war in the future.
[29] Kish, 146.
[30] Geneva Convention IV, Art. 5, August 12, 1949, in Roberts and Guelff, *Documents on the Laws of War*, Oxford University Press, 2004, p. 303.
[31] International Committee of the Red Cross, Commentary to Article 46 of 1977 Geneva Additional Protocol I, p. 566, <http://www.icrc.org/ihl.nsf/COM/470-750056?OpenDocument>.
[32] *Customary International Humanitarian Law*, ICRC, Jean Marie Henckaerts and Louise Doswald-Beck, eds., Vol. 2: Practice, Cambridge University Press (2005), p. 2568.
[33] The ICRC was founded in 1863 in response to the carnage at the Battle of Solferino between France and Austria. The organization has a unique legal status under international law; the 1949 Geneva Conventions mandate that the ICRC train armed forces to respect the laws of war and to develop and extend the Geneva Conventions.
[34] *Customary International Humanitarian Law*, ICRC, Jean Marie Henckaerts and Louise Doswald-Beck, eds., Vol. 2: Practice, Cambridge University Press (2005), p. 2568.
[35] Hague Convention Regulations Respecting the Laws and Customs of War on Land, Art. 24, October 18, 1907.
[36] Kish, 125.
[37] Maj. Richard Baxter, "So-Called 'Unprivileged Belligerency': Spies, Guerrillas, and Saboteurs," *The British Yearbook of International Law*, 1951, p. 331.
[38] Hague Convention Regulations Respecting the Laws and Customs of War on Land, Art. 24, October 18, 1907.
[39] International Committee of the Red Cross, Commentary to Article 46 of 1977 Geneva Additional Protocol I, p. 562, <http://www.icrc.org/ihl.nsf/COM/470-750056?OpenDocument>.
[40] John Kish, *International Law and Espionage*, Martinus Nijhoff Publishers, 1995, p. 148.
[41] *Customary International Humanitarian Law*, ICRC, Jean Marie Henckaerts and Louise Doswald-Beck, eds., Vol. 2: Practice, Cambridge University Press (2005), p. 2568.
[42] *Customary International Humanitarian Law*, ICRC, pp. 2569, 2572.
[43] *Customary International Humanitarian Law*, ICRC, p. 2571.
[44] As stated earlier, these justifications—and this paper's argument that the laws of war should grant prisoner-of-war status to captured war spies—only apply to spies who are not citizens or nationals of the state that captured them. There is a powerful independent justification—which this paper does not attack—to deny prisoner-of-war status to those spies: they are properly considered traitors, and it can be safely presumed that no state will be willing to abdicate its sovereignty and grant prisoner-of-war protections to them.
[45] Olson, 15-31.
[46] Olson.
[47] Olson, 17-18.
[48] Olson, 24-25.
[49] Olson, 24-25.
[50] William Edward Hall, *A Treatise on International Law, 6th Edition.* J.B. Atlay, ed., Oxford, 1909, p. 535.
[51] Henry L. Stimson and McGeorge Bundy, *On Active Service in Peace and War*, Harper, New York, 1948, p. 188.
[52] Olson, 15-17.
[53] Olson, 20-22.
[54] Olson, 27-29.

[55] "The Death of John Andre," Spy Letters of the American Revolution Collection, Clements Library, University of Michigan, <http://www.si.umich.edu/spies/stories-arnold-4.html>.
[56] Stimson and Bundy, p. 188.
[57] Olson, 34.
[58] Olson, 18-20.
[59] J.M. Spaight, *War Rights on Land*, London, 1911, p. 205 (quoting Colonel A.L Wagner, Service of Security of Information, p. 181).
[60] P.K. Rose, "The Founding Fathers of Intelligence," Center for the Study of Intelligence, Central Intelligence Agency, 1999, <https://www.cia.gov/csi/books/940299/art-1.html>.
[61] Rose, <https://www.cia.gov/csi/books/940299/art-1.html>.
[62] Michael Gordon, "German Intelligence Gave US Iraqi Defense Plan, Report Says," *The New York Times*, February 27, 2006. <http://www.nytimes.com/2006/02/27/politics/27germans.html?ex=1298696400&en=f01b49420a09578d&ei=5088>.
[63] Charles Hawley, "Berlin's Spies Reportedly Helped US," *Spiegel Online*, January 12, 2006. <http://www.spiegel.de/international/0,1518,394874,00.html>.
[64] *Sun Tzu on the Art of War, Lionel Giles, trans., May 1994.* Accessed November 15, 2006, at <http://www.fas.org/man/artofwar.htm>.
[65] Stephen E. Ambrose, *D-Day: The Climatic Battle of World War II*, Simon & Schuster, New York, 1994, pp. 77-84.
[66] Toni Pfanner, "Military Uniforms and the Law of War," *IRRC* 86, No. 853 (March 2004), p. 119. See, e.g., Australia Defence Force Manual (1994) ("normally"), paragraphs 512-513; United Kingdom LOAC Manual (1981) ("usually), Section 3, p. 9, paragraph 2.
[67] Remarks by Judge Abraham D. Sofaer, Legal Advisor, U.S. Department of State, at the Sixth Annual American Red Cross-Washington College of Law "Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions," published in *American University Journal of International Law and Policy*, Vol. 2, 1987, p. 466. Also quoted in Toni Pfanner, "Military Uniforms and the Law of War," *IRRC* 86, No. 853 (March 2004), p. 119.
[68] Confining the horrors of combat to lawful combatants, a critical objective of the laws of war, is supported by both the principal of distinction and the principle of proportionality. The latter, as codified in Additional Protocol I to the 1977 Geneva Conventions, prohibits military attacks that cause incidental civilian casualties or damage to civilian objects that is excessive in relation to the anticipated direct military advantage of the attack.
[69] Herfried Munkler, "The Wars of the 21st Century," *IRRC* 85, No. 849 (March 2003), pp. 8-10.
[70] Whether espionage tends overall to prolong or limit warfare (in scope, duration, or intensity) is admittedly an empirical question beyond the scope of this article. Still, as long as espionage does not necessarily prolong warfare, opponents of greater protection for war spies must find other bases for support.
[71] See, e.g., Kal Raustiala, "Compliance and Effectiveness in International Regulatory Cooperation," *Case Western Reserve Journal of International Law*, 32 (2000), p. 387, in which Raustiala argues that compliance methods can be counterproductive to achieving effectiveness.
[72] 1977 Geneva Protocol I Additional to the Geneva Conventions Article 51.5(b), June 8, 1977, p. 449, in Roberts and Guelff, *Documents on the Laws of War*, Oxford University Press, 2004, p. 449.
[73] This argument not unreasonably assumes that captured war spies and saboteurs share the same end—execution—in states that have the death penalty (or that use it during conditions of war or martial law). State practice in the 20th century overwhelmingly supports this assumption. A detailed review of national laws on this topic is beyond the scope of this article.
[74]Recent state practice, both in the public statements of government ministries and the conduct of their armed forces, leaves no doubt of the importance of the principle of distinction. In July 2006, the Israeli Ministry of Foreign Affairs—responding to criticism from a number of NGOs including Human Rights Watch—issued a formal statement that defended the Israeli Defense Force's efforts to distinguish between combatants and civilians in Lebanon and strongly criticized Hezbollah for indiscriminate attacks on Israeli civilians. *See* "Responding to Hizbullah Attacks from Lebanon: Issues of Proportionality," Israel Ministry of Foreign Affairs, July 25, 2006, at: <http://www.mfa.gov.il/MFA/Government/Law/Legal+Issues+and+Rulings/Responding+to+Hizbullah+attacks+from+Lebanon-+Issues+of+proportionality+July+2006.htm>.
U.S. forces in Iraq have made significant efforts to distinguish combatants from civilians. Prior to their assault on Fallujah in November 2005 with as many as 15,000 troops, U.S. Marine and Army forces surrounding the insurgent stronghold launched an extensive information campaign urging civilians to leave and gathered a trove of specific intelligence on insurgent hideouts within the city. An estimated 250,000 civilians (almost 90 percent) fled before the attack, which destroyed almost half of Fallujah's 39,000 buildings. See Colin H. Kahl, "How We Fight," *Foreign Affairs*, Vol. 85, No. 6, November/December 2006, p. 9.

Neil Beck is a national security lawyer working for the U.S. government.

Remembering Tom Dillon

April 25, 1932 - January 22, 2011

by COL (Ret) Michael M. Ferguson, with Contributions from Other Colleagues

Mister (LTC and SES, Retired) Thomas Dillon's 48 years of government service began with his enlistment in the U.S. Army on 29 April 1955. Following basic and advanced Infantry training and assignment to the 1st Infantry Division at Fort Riley, KS, he was quickly selected for Officer Candidate School. Upon graduation from 51st Company, Fort Benning, GA, on 29 May 1956, he was commissioned a 2LT of Infantry. Tom went on to Airborne and Jumpmaster Schools and was assigned as the Executive Officer, Service Company, Berlin Command, Germany. He returned to the U.S. in 1959 and served as an Infantry Platoon Leader in the 101st Airborne Division at Fort Campbell, KY, until his selection for counterintelligence training. Following a stint from 1960 to 1961 as Senior Agent in Charge, 109th CI Group, Louisville, KY, Tom was cross-trained in HUMINT and posted to U.S. Army Europe's 513th Military Intelligence Group, with duty station Munich. For the next three years he led teams conducting HUMINT collection against the Soviet Union and other Warsaw Pact nations. Tom returned to CONUS and joined the U.S. Army Intelligence and Security Command Operations Staff at Fort Holabird, MD. He was then chosen by name to form a HUMINT Collection Company at Fort Bragg, NC. He took the company to Vietnam, where he and his soldiers were responsible for HUMINT, commanding it during its deployment to that war-torn country. Returning to Germany in 1967, Tom served for two years as the Operations Officer, Berlin Detachment, 513th MI Group, and then returned to Munich where he commanded a detachment of the 66th MI Group until 1970 when he was selected for the U.S. Army Command and General Staff College.

At this point Tom had 15 years service, of which fully 11 years were in operational HUMINT or CI positions—most of it as a commander or a team leader. He had already

earned a significant reputation as a superior officer, mentor, and partner with his colleagues, counterpart services, and the men and women who worked for him. COL (USA, Ret) Stu Herrington recalls then-MAJ Tom Dillon as his first boss on active duty and his comments below underscore Tom's mentoring style and commitment to doing the right thing—all the time.

I was fresh from the Area Studies course, and because I'd been in grad school for three years, the Army had made me a 1LT before I entered active duty in 1967. I arrived in Berlin in April 1968 and was promoted within three months (having been on active duty a total of one year). I was really too green to be a captain, but that was the system back then. Tom looked out for me and kept me in check. Tom was a laid-back, smart, decent fellow, fluent in German and well-liked. He sent me to German language school in Oberammergau for the 5-week advanced course, even though I didn't speak a word of German. His reason? "The old man will let you go for five weeks, but not for the basic, 14-week course, so you'll have to work hard to play catch-up ball, but the alternative is no school." I served under Tom during that Berlin tour and loved the MI business. However, Vietnam and a wife who didn't like the Army so well induced me to separate and try the civilian world. At that time, Tom counseled me that he believed I was made to be an MI-HUMINT officer, and that he felt certain I would not be happy working for corporate America. He put me in for an ARCOM, in those days rarely done for 2-year guys who were getting out, and told me, "We wish you the best, but if I'm right and you are not satisfied with civilian life, the road back is open. Your record and our recommendation (in an ARCOM, an OER, and a farewell letter) should enable you to reenter active duty. Don't be too proud if you realize you made a mistake." Within four months (having taken a job and, as Tom predicted, hating it), I was on the phone to MI Branch telling them, "You've got to get me back on active duty. I'll go to Vietnam, anywhere, just check my file and you'll see that this is the right thing to do." Long story short, they got me back on AD on 30 June 1970, the last day of the then-fiscal year for which there were funds to recall officers into an Army that was being drawn down. Were it not for Tom and the gracious manner he treated me at that critical moment, I probably would not have come back on active duty. It would have been easy for Tom to have written me off as someone who spurned the Army, not put me in for that ARCOM, and not said the things he said to me. I know his manner of handling me during that conflicted time changed my life.

Completing CGSC as an honor graduate, Tom returned to Vietnam for his second tour where until 1972 he commanded a provisional battalion responsible for all Army CI and HUMINT operations throughout the country. With the end of the war in sight, Tom was reassigned to Bangkok, Thailand, as the Deputy Commander, Detachment K, 500th MI Group—responsible for Army HUMINT collection operations throughout Southeast Asia—until 1975 when he retired from the Army as a lieutenant colonel. Tom's entire career was peppered with episodes that may have been less dramatic than that described by COL Herrington below, but were based on the fact that Tom believed that the Army and its leaders—military or civilian—took care of their own. To Tom, no operational or personnel issue was too large to tackle or too small to ignore.

It seemed that wherever I was assigned after that, there was Tom. In Vietnam, I was with MACV, while he was there with the 500th. We met several times in Saigon, and Tom met Thuan, the Vietnamese woman who would later become my wife. When it started to look like a cease-fire and U.S. withdrawal was in the cards, Tom approached me in Saigon to ask, "What are you going to do about Thuan?" who was pregnant at the time. I told him that I was on orders for the Advanced Course at Fort Huachuca, and would be sending her money while in CONUS, and then would see if I could get back, if not to Vietnam, somewhere close. Tom, who remained in Saigon, volunteered to look out for her if she needed help. Less than a year later, I was reassigned to the Embassy in Saigon, and Thuan was there, having given birth to twins. Due to the cease-fire, Tom had been forced to relocate to Bangkok, but came to Saigon regularly. I did mini-R&R at his Bangkok villa a couple of times in 1973 and 1974, and things perked along until the North Vietnamese Army started knocking on Saigon's door. Predictably, there was Tom on my doorstep to ask, "What about Thuan and the kids?" (There was now a son as well.) "Do you have a plan to get them out?" I told Tom that I had them all in Saigon, and the plan (since we had just married that week, in early April 1975) was to keep them close, and hope that, during any evacuation, I could slip them into the flow of refugees, and we could reunite later, when I was done working the evacuation. Tom told me, "That's too risky, you could lose them. Can you get them on a C-130 to Utapao?" (I was on the U.S. Delegation to the Four Party Joint Military Team in Saigon, and we had a weekly C-130 flight to Hanoi, that did not stay overnight in Saigon upon return but rather, due to the limit of 50 military personnel in Saigon, had to drop us off, then fly to Utapao.) Tom told me, "Get them on the C-130 to Utapao next week, let me know they are inbound, and leave the rest to

me." When they arrived in Thailand, they were met by Tom and whisked out the gate. The destination was Tom and Betty's villa in Bangkok, where the Dillons safe-havened my bride and three babies for two months, which is how long it took me to depart from the Embassy roof, get off the carrier of TF 75, transit the Philippines en route to Bangkok, then persuade the U.S. Embassy in Bangkok to legalize my new family. We named our son "Thomas," after Tom, and Tom named his first-born "Travis Herrington Dillon." Our kids knew him from the beginning as "Uncle Tom," and loved him immensely. At Tom Dillon's Arlington service, after everyone had left the graveside site, my Tom stood in silent prayer over his Uncle Tom.

LTC Dillon retired from the Army in 1975, but soon returned to his nation's service as a member of the Military Intelligence Civilian Excepted Career Program (MICECP). In this capacity he was again assigned to Germany. Between 1976 and 1985 Mr. Dillon served as a CI staff officer, Headquarters, U.S. Army Europe, in Heidelberg; Operations Officer, 66th MI Group, in Munich; and from 1981 to 1985 as the Senior U.S. Army Europe Intelligence Liaison Officer to the Federal Republic of Germany. In 1985 Tom returned to the United States to attend the Army War College at Carlisle Barracks, PA. He was then named HUMINT Advisor to the Deputy Assistant Secretary of Defense (Intelligence) (ASD/I) at the Pentagon. He performed this role until 1989, providing oversight on all Defense HUMINT activities and developing new policies regarding HUMINT support to drug interdiction and special operations. This experience would serve him well in his later postings at the executive level within DIA and the Defense HUMINT Service. In 1989 Mr. Dillon returned to Germany, this time as the Special Assistant to the Deputy Chief of Staff for Intelligence, U.S. Army Europe. With the fall of the Soviet Union and breakup of the Warsaw Pact, HUMINT efforts in Europe posed unique challenges and opportunities for Army collection efforts. The changing U.S.-German relationship in the turbulent 1980s and early 1990s greatly exacerbated these challenges. Dillon was the Army's key player in managing this unique and evolving relationship, personally working with senior German intelligence and security officials to guide the relationship to ever more productive joint endeavors.

COL (USAR, Ret) Bill Halpin first met Tom in 1976 shortly after Tom's retirement from the Army. Halpin was also a MICECP officer and interacted with Tom during their mutual tours in Germany and later while assigned together to DIA in Washington. COL Halpin comments on Tom's professionalism, credibility, and steady hand in often tense and sensitive circumstances:

In 1991-94 our relationship deepened. As the West Berlin scene settled, I was reassigned to Heidelberg as the Chief, Collection Division. Although we were the same GS grade, Tom became more of a mentor to me there. He became my confidant and I learned to appreciate his sage advice and wisdom. He always seemed to possess the critical piece of "insider" information I needed to succeed. In 1988 I was assigned to West Berlin when Tom became the Special Assistant to the Deputy Chief of Staff for Intelligence, Headquarters, U.S. Army Europe. Between 1989 and 1995, Tom and I worked several issues together, as some of his direct reports were assigned to projects in West Berlin. After the fall of the Berlin Wall in 1989, the Berlin Commander became concerned about the continued relevance and presence of at least one very sensitive and controversial special project. As the senior DoD intelligence officer in Berlin, the Commander and Chief of Staff frequently challenged me about this project. Naturally, I'd call on Tom. He'd travel to Berlin to explain why the particular project could not be dismantled. I was impressed by his uncanny ability to solve complex personnel and operational challenges. He was the genuine "gray eminence behind the curtain," pulling the strings that calmed the waters. When the U.S. Military Liaison Mission (USMLM) was disestablished in 1990, Tom was instrumental in preserving employment and transfer of a dozen or more assigned civilian analysts to West Germany. This success was attributable to Tom's close professional associations within the senior-most tiers of the West German intelligence services.

Tom Dillon's efforts were widely acknowledged in the highest circles and resulted in his being awarded the Gold Cross of Honor from the Federal Republic of Germany in 1995. The Cross of Honor, also known as the Honor Cross or, popularly, the Hindenburg Cross, was a commemorative medal inaugurated on July 13, 1934, by Reichspräsident Paul von Hindenburg for those soldiers of Imperial Germany who fought in World War I. Upon returning to the United States, Tom was assigned to DIA where he served as Chief of Plans, Programs, and Policy, Directorate of Operations, and was designated as the lead in the transition and establishment of the Defense HUMINT Service (DHS), which he headed for three years as its first Executive Director from 1997 to 2000.

Mr. Dillon's extraordinary operational accomplishments in reshaping worldwide HUMINT operations made critical contributions in such priority areas as U.S. assessments of Russian and Chinese weapons of mass destruction (WMD). These weapons are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. WMD can be high explosives or

nuclear, biological, chemical, and radiological weapons. Tom was also involved in the protection of U.S. interests from terrorist activities, information operations, and "on-the-ground" intelligence support to deployed forces in Bosnia, Kosovo, and East Timor. In Bosnia, he deployed DH operational personnel before the signing of the Dayton Accords in order to prepare the U.S. sector for the introduction of peacekeeping forces. He then constructed a complex and highly effective collection capability in the region to ensure the safety of U.S. forces.

Shortly after returning to the U.S. Army as Director of Counterintelligence, HUMINT, Security, and Foreign Disclosure in the Office of the G2, Tom recognized the demands that the Global War on Terrorism (GWOT) would place upon the Army's tactical forces. He moved quickly to reconstitute an organic Army HUMINT capability, which had been largely disestablished after the standup of DHS in 1995. He secured the necessary resources to allow immediate reestablishment of this asset. This reinvigorated capability, known as the Army Operational Activity, achieved an initial operating capability in early 2003. During this period Mr. Dillon also spearheaded a complete transformation of the Army's CI efforts. In cooperation with the newly established Counterintelligence Field Activity (CIFA)[1], sister services, and other U.S. agencies, he implemented several major initiatives including establishment of worldwide CI Force Protection Detachments to work with host nation intelligence and security services in providing crucial force protection information to troops in transit through potentially hostile regions. Another contribution was the placement of Army CI agents in the FBI's Joint Terrorism Task Forces (JTTFs) throughout the United States, enabling a complete interagency effort to be brought to bear in the GWOT.

Another illustration of Mr. Dillon's achievements was his establishment of the Army Research and Technology Protection Center (ARTPC). The ARTPC mission is to ensure that critical enabling technologies are safeguarded from exposure and that the U.S. military maintains its technological edge over all adversaries. This has become the model throughout DoD (**D**ial **O**n **D**emand)[2] on how to provide an integrated effort to ensure the safeguarding of critical technologies. Combining CI, security, and engineering expertise into one organization, the ARTPC brings together the research and development (R&D), acquisition, and CI communities in order to identify and protect critical technologies from compromise early in their life cycles.

The challenges enumerated above could easily have consumed the total attention of a lesser man, but to Tom they seemed simply to be things that needed to be done—and he did them with panache, compassion and, as COL Bill Halpin attests, that constant concern for others that was his hallmark:

> *In August 1994 as a prelude to the establishment of the Defense HUMINT Service, I was transferred to DIA to manage HUMINT operations. Shortly thereafter, Tom arrived as the Executive Director. Again, Tom served as guide and mentor. During some particularly troubling times, he frequently reminded me not to be concerned about things that cannot be controlled. He once talked me out of leaving the organization, reminding me boxers sometimes retreat to their corners and cover up until the opponent tires. In August 1999, I was ready to move and Tom facilitated my transfer to what was to become the best assignment of my career.*

While at DIA and later with Army G2, Tom was often characterized as "singularly responsible" for fostering unprecedented cooperation among DIA, the Army, and sister intelligence organizations. He worked closely with CIA, NSA, NGA (then NIMA), and NRO to forge partnerships which greatly improved the level of commitment, integration, and effectiveness of joint operations. Mr. Dillon also partnered with many foreign governments in the establishment of joint, multilateral, and bilateral collection programs that resulted in the furthering of U.S. national objectives. Tom's unique ability to quickly and effectively interact professionally, and as a genuine American, with foreign partners beyond Germany is illustrated by COL Don Fox:

> *In January 2000, Tom, then the Executive Director of the Defense HUMINT Service, formed an assessment team with the late LTG Sidney T. Weinstein (former Army Deputy Chief of Staff for Intelligence) and LTG (Ret) James A. Williams (former Director, DIA) for a 12-day trip to the Far East to review the mission capabilities and performance of Field Operating Bases (FOBs) and Defense Attaché Offices (DAOs) in five countries. As Chief of FOB-Korea, I welcomed this high-level visit from such an esteemed trio of intelligence legends and knew that they would enjoy their short visit to the Land of the Morning Calm. Their arrival coincided with our annual New Year's reception at U.S. Army Garrison (USAG) Yongsan, to which the majority of senior U.S. and Republic of Korea (ROK) intelligence professionals (and for the first time the CINC, U.S. Forces Korea (USFK), GEN Thomas Schwartz) were to attend. I met Tom and the assessment team at Kimpo International Airport in Seoul with a carefully crafted speech that had been prepared for him to deliver at the reception. Tom briefly reviewed the speech and then focused his attention on learning more about the guests and any issues that might surface during the biggest annual*

DIA social event in the ROK. We arrived just in time to change clothes and form the receiving line, where I then watched Tom work his magic. He was in complete control of his environment and skillfully demonstrated his keen intellect and charming personality with everyone in attendance. Tom spoke expertly using his interpreter/translator support as if he had rehearsed it for hours and worked the crowd like a true professional—ensuring everyone felt that they were both appreciated and necessary to our mutual interests. The FOB-K New Year's reception was far more successful than I could have imagined because of Mr. Dillon's supportive and impressive performance. It was a huge morale boost for FOB-K and, for the remainder of my tour of duty as Chief of FOB-K, I consistently received laudatory comments from senior ROK officials for Mr. Dillon's lasting impression—an impression that those of us who were fortunate to have worked with Tom also share.

With a career spanning over four decades, Tom Dillon retired from the U.S. Army Senior Executive Service in 2004. He immediately joined Phoenix Consulting Group (later DynCorp, Intl.) as a senior consultant and continued to educate, mentor, and set an example for another decade's worth of young intelligence professionals receiving training from that organization until his passing on January 22, 2011.

Tom was a whole person and no description of him or his deeds would be complete without understanding his deep commitment and love for his family and his close friends—a commitment and love that was reciprocated in full. He met and married the love of his life, Betty, while in Germany early in his career, and those of us who knew them well understood that he would not be long in following her passing to eternal life in November 2010. His garden, the cats, his books, good food, good wine, and the ability to contribute in a meaningful way were everything to him. Nevertheless, Betty and their children Patrick and Maureen were the core and soul of Tom's life and being. Maureen's comments at her father's funeral mass captures his love of family and their love for him:

My brother and I want to thank everyone for coming and for all of your kind words during this difficult time. A lot of you knew my father through work and became good friends and colleagues. My brother and I knew a different man. We knew our Dad. The Dad that was proud of us no matter what. The Dad that believed in us when we didn't. The Dad who would get up at night and feed me when I was a baby so my Mom could sleep. The person we trusted above all others. Whose hands were always warm even in the winter when it was freezing outside. He was also the man who told me one night when my Mom was sick that he wanted to marry her. I told him that they were already married but he told me that he wanted to get re-married by a priest. The day that my mother died, my parents were married; my mother was baptized and was given the Anointing of the Sick. During my mother's illness, I saw my parents as I had not seen them before. I saw two people who truly loved each other. I can only hope that someday I will be as lucky to experience that level of devotion. We miss you, Dad, and we will love you forever.

Stu Herrington was one of Tom's closest friends and concluded his remembrance as follows:

To me and my entire family, Tom Dillon was a guardian angel, a terrific friend, and a steadfast supporter and mentor of mine. None of us will ever forget him or Betty. I took a picture of Tom in Bangkok in 1974 when he came home from work in his Class B Army uniform, with ribbons, the only time I ever saw him in uniform. Years later, I made an 8 x10 of that shot and gave it to Tom and Betty, it being so rare a glimpse of a uniformed LTC Dillon. I was proud that this picture was prominent in the slide show that we saw at the service in the funeral home. It has hung on my office wall for 15 years, and still is there, evoking Tom's memory every day. God bless a great man.

My own experience with Tom also covered 15 years and has left me with a mental picture I will try to put in words:

A consummate professional, Tom was a man who was devoid of sham. I never saw him visibly angry or upset nor heard him curse (and do not know anyone who did either). He was a man of great character, integrity, and courtesy and a man of considerable grace—I never knew him to talk with anyone without coming out from behind his desk. He always stood whenever a woman entered the room, and when he met you he smiled that winning smile. He listened—more importantly he heard and understood! Tom had infinite patience and a remarkable ability to influence people—always for the greater good. He never used the word "I" when referring to a success and never the word "they or you" when explaining why on those rare occasions something may not have turned out successfully. Simply put, if I could choose the man my son would become, it would be pretty close to Tom Dillon.

We buried this soldier, leader, mentor, and father at Arlington National Cemetery on 11 May. In addition to his children, his sisters Maureen Prior and Margaret Tine, and other family members, two former Directors of DIA, the

Army G2, and a score or more of retired and active senior officers and DoD civilians attended to honor his memory. He was a man who became part of one's experiences—always in a good way and always worthy of emulation; he was a man who mattered—a man who made a difference—and that was reflected in those who were there for the final rendition of Taps played in his memory. It is of no small significance that a hundred or more of those present were civilian and military staffers who had worked for Tom—the folks who were captains, majors, and mid-grade civilians when Tom Dillon touched their lives.

The Mass was (as Tom would have approved) short and to the point, and the performances of the Old Guard, the black horse caisson, the band, and the bugler were superb. I rode with LTG (USA, Ret) Pat Hughes to the gravesite in the cortege following the service and we talked of the ceremony, the honor, and the distinction that interment at Arlington means to those who keep the military faith. Arriving at the site we were both struck (but not too surprised) to discover that Tom had managed to arrange for a spot near the only shade tree for at least 100 yards in any direction. We stood with the others in the sun, on a red dirt path, and listened to the three volleys from the riflemen followed by the plaintive notes of Taps, which as always brought me close to tears, when from the direction of the Pentagon came the unmistakable "whop-whop-whop" of a UH-1 lifting off. I—and I'm sure more than a few other Vietnam vets—had a bit of a flashback moment. Then I smiled and reflected on how appropriate it was to have a Huey flying over Tom's last PZ—I'm sure that Tom was smiling too.

What you leave behind is not what is engraved in stone monuments,
but what is woven into the lives of others.
- Pericles

Notes

[1]Counterintelligence Field Activity (CIFA) was a United States Department of Defense (DoD) agency whose size and budget were classified. CIFA was created by a directive from the Secretary of Defense (Number 5105.67) on February 19, 2002. Recently, CIFA was incorporated into the Defense Counterintelligence and HUMINT Center at DIA.

[2]A feature that allows a device to automatically dial a telephone number. For example, an ISDN router with dial on demand will automatically dial up the ISP when it senses IP traffic destined for the Internet.

Michael M. Ferguson, Colonel, U.S. Army (Ret), is the principal author of this memorial article. As a platoon sergeant with nine years enlisted service, he was selected for OCS and commissioned in the Infantry in 1970. His troop assignments include the 44th Medical Brigade; the 1st, 4th, & 7th Infantry Divisions; and the 3d Armored Division. He has also served on the European Command and Allied Land Forces Southeastern Europe (NATO) staffs. He served 25 years as a Foreign Area Officer and is a recognized expert on African affairs, with broad interagency experience, five tours in Africa as a Defense Attaché (Ethiopia, South Africa, Tunisia, and Cameroon), and service as the Special Assistant for African Affairs to the Assistant Secretary of Defense for International Security Affairs. COL Ferguson also served two years as the first Chief of HUMINT Training and Professional Development for DIA/DHS, with concurrent duty as the Dean of the Defense Attaché School and additional responsibility for the STC program and the Defense Debriefing School. He retired in 2001 with 40 years of service. COL Ferguson is a life member, President Emeritus, and Director of the Foreign Area Officer Association. He is a member of the U.S. Defense Attaché Hall of Fame, the Infantry OCS Hall of Fame, and the Board of Directors, NMIA.

Stuart A. Herrington, Colonel, U.S. Army (Ret), is an author and retired CI interrogator. His 2003 audit of conditions at the Abu Ghraib prison in Iraq prompted scrutiny of U.S. interrogation efforts in the Global War on Terror. He joined Military Intelligence branch in 1967 and served in Berlin before deploying to Vietnam in 1971. Herrington served in the Defense Attaché Office in Saigon and was among the last Americans to helicopter off its roof when the city fell to the North Vietnamese Army in 1975. He spent most of the next decade with Army CI in Berlin and played a role in the arrest of more than a dozen spies in the Clyde Lee Conrad Ring that had been selling NATO war plans to the Russians. After Operations JUST CAUSE (1989) and DESERT STORM (1991), Herrington led the interrogations of high-value detainees. From 1992 to 1998, he was Director of DIA's Asia/Pacific Division, commanded the U.S Army Foreign Counterintelligence Activity, and supported the U.S. Task Force Russia probe into the fate of Cold War POWs/MIAs. COL Herrington retired from the military in 1998.

Don A. Fox, Colonel, U.S. Army (Ret), received his commission in 1976 as a Distinguished Military Graduate in the Reserve Officer Training Corps from Appalachian State University. He served as a CI and HUMINT officer in a wide range of assignments at Fort Huachuca, AZ; Fort Bragg, NC; Fort Meade, MD; the Republic of Korea; and in Southwest Asia during Operations DESERT SHIELD and DESERT STORM. From 1994 to 1999, COL Fox managed the U.S. Army MI Excepted Career Program during the transfer of military service strategic HUMINT authorities to the Defense HUMINT Service, DIA. From 1999 to 2000 he served as Chief, Field Operating Base-

Korea, Defense HUMINT Service, DIA/DHS, until his final assignment in 2000 as Commander, INSCOM Training and Doctrine Support Detachment, Fort Huachuca, AZ, where he retired from the U.S. Army in 2003. Don is employed by Six3 Systems, Inc., as a CI and HUMINT subject matter expert.

William R. Halpin, Colonel, U.S. Army and DoD Civilian Intelligence Officer (Ret), served 20 years of his 30-year career overseas in Europe and Asia. His assignments included all aspects of HUMINT field operations as well as staff positions of increasing scope and responsibility, culminating in serving as the principal staff officer and operational program manager for worldwide HUMINT. He also had a concurrent 31-year U.S. Army Reserve career in HUMINT and special operations, which included assignments with the 149th MI Battalion and the 5th Special Forces Group in Vietnam, the 430th MI Battalion in Europe, and Reserve active duty assignments with the Joint Special Operations Activity, U.S. Special Operations Command, European Command, DIA, and INSCOM. COL Halpin also served as an attaché to the United Kingdom and commanded at the brigade level. From 1999 to 2008, Mr. Halpin helped educate future leaders of the intelligence and national security communities at our nation's center of excellence, the National Defense Intelligence College. He held the Wilson Chair for Intelligence Studies, and taught courses related to four collection disciplines and analysis. After five years as a HUMINT Mission Manager with Northrop Grumman Mission Systems, Mr. Halpin established SIS Consulting, Inc., and has been the owner and managing director since 2008. He is a member of the Infantry OCS Hall of Fame and holds the MI Corps' Knowlton Award for career excellence. He is also a member of the Board of Directors, NMIA.

Into the Crucible:
Intelligence Leadership Challenges at the Tactical Level

by MAJ (USA) Joseph T. Kosek, III

In the *Harvard Business Review* article "Crucibles of Leadership," authors Warren Bennis and Robert Thomas describe a crucible experience as "a transformative experience through which an individual comes to a new or an altered sense of identity."[1] My crucible experience began in June 2006 and came in the form of growing a 40-person Military Intelligence Company (MICO) into a 72-person MICO and preparing the company for combat in six months. I accomplished this monumental task by beginning with the end in mind, establishing benchmarks, listening to my subordinates, and never losing focus. As a result of this crucible experience, I learned that if I am truly focused on obtaining a goal, nothing can stop me, and even the most insurmountable challenge is achievable when it is broken down and accomplished in smaller portions.

My crucible experience began on June 30, 2006, as I stood on a parade field on a picturesque summer day at Fort Bragg, NC. Around me, friends and family watched as I took command of the MICO for the 4th Brigade Combat Team, 82nd Airborne Division. I was ecstatic because, at 26 years of age and in the 82nd Airborne Division for just one year, I had beaten out several other older and more experienced captains to take command of the MICO. Everything seemed perfect at the time, even if the company possessed only 40 of the required 72 personnel in formation. I had no idea what lurked immediately beyond the horizon, however.

A month after I assumed command, the 4th Brigade Combat Team received orders to deploy to Afghanistan. As a result, I now faced a monumental task – to get the remaining people and equipment that the MICO needed and train the company to perform its wartime mission in six months. To fully understand the complexity of the situation, one must first understand the company itself. The MICO breaks down into four separate sections: an Unmanned Aerial Vehicle (UAV) unit, a Signals Intelligence (SIGINT) unit, a Human Intelligence (HUMINT) unit, and a Headquarters (HQ) unit. In June 2006, the UAV unit possessed four of the required 23 personnel and none of its required equipment. The SIGINT unit maintained 50 percent manpower strength and a small portion of its required equipment. The HUMINT and HQ units represented the strongest sections of the company, both with over 50 percent of their required personnel and all of the required equipment. While the HUMINT and HQ units appeared the strongest on paper, every section lacked the training necessary for Afghanistan, making the toughest early challenge figuring out where to apply command emphasis and when. The fact that I lacked a senior intelligence officer in my direct chain of command only compounded this problem.

Under the Army's modular brigade system, the MICO served a Brigade Combat Team (BCT) as a subordinate unit of the Special Troops Battalion (STB). The STB represented an "enabler" battalion for the BCT, as the three principal companies of the STB – the engineer company, the military intelligence company, and the signal company – enhanced the ability of the remainder of the BCT. According to the Army's design for the STB, the top three leaders in the unit – the Battalion Commander (BC), the Executive Officer (XO), and the Operations Officer (S3) – should each represent a branch of one of the subordinate companies, either Engineer branch (EN), Military Intelligence (MI) branch, or Signal Corps branch (SC). The Army conceived the STB leadership structure with the notion that if the BC, XO, and S3 possessed an intimate understanding of subordinate units, the top three could better plan appropriate training, develop junior leaders, and tactically employ each company. Unfortunately, when the Army first introduced this concept, the EN, MI, and SC branches lacked the required number of field grade officers to fill every BC, XO, and S3 role in each STB. This meant that field grade officers from other Army branches who lacked the requisite subject matter expertise filled the void.

In my STB the BC was an Engineer officer, but the XO was an Air Defense Artillery officer and the S3 was an Infantry officer. The ramifications of this manning slate meant that, as a captain who converted to MI only 18 months prior, I now represented the senior-most intelligence officer within the STB and the second senior-most intelligence officer in the BCT. As my battalion leadership had offered no immediate solutions for preparing my intelligence soldiers to perform their branch-specific mission in combat, I

needed to look outside the battalion for answers to questions regarding intelligence training, while simultaneously leveraging the company's internal strength.

I then turned to the Brigade S2 (BCT S2), or senior-most intelligence officer in the BCT, for assistance. While the BCT S2 showed a willingness to help, his capability to do so was limited as he never previously deployed as an MI officer, never commanded an MICO, and spent the last three years away from the tactical environment teaching Reserve Officer Training Corps (ROTC) cadets. Moreover, the BCT S2 needed to focus on filling his own manning shortages and achieving his section training objectives. Within the company, my second in command, or Executive Officer (XO), and my First Sergeant (1SG) represented my two primary helpers in preparing the company for deployment. Similar to the BCT S2, both showcased a willingness to help, but both lacked the extensive tactical MI resumé to counter my inexperience. Neither my XO nor my 1SG had deployed previously and my 1SG returned to tactical MI duties only two months before, after serving as a Drill Instructor for a number of years. Additionally, my XO recently married and my 1SG's wife just gave birth to a newborn girl, thereby drawing a considerable portion of both of their focuses away from the primary mission at hand. This only added to my growing list of leadership challenges.

After fully ascertaining the severity of the challenges I faced, I was severely tempted to fold. I felt the complexity of the tasks the MICO needed to perform in Afghanistan, given the current manning and equipment shortages, was simply a bridge too far. I believed the company could not attain the overall level of pre-combat deployment readiness necessary in the time allotted. Moreover, as the Company Commander, I felt incredibly overwhelmed and underprepared, like someone had dropped me in the middle of the Atlantic Ocean without a raft or life vest and expected me to swim home. Exhausted, at one point I sat down to try and collect my thoughts and regroup before continuing the fight. During this time, I came to a relatively simple, yet startling, realization. I realized the Army would eventually provide me with more personnel and equipment; the only thing I did not know was when the Army would provide those resources. Therefore, I soon surmised that instead of dwelling on my own or the MICO's shortcomings, or when the Army would deliver the people and equipment I desperately needed, my time was better spent focusing on what we did have and how to make it work.

I began by determining the missions the MICO needed to perform in Afghanistan and the pre-deployment training requirements necessary to accomplish these tasks. The UAV unit flew over large portions of ground to determine enemy positions. The HUMINT unit talked to local nationals to try and find enemy safe havens and identify key enemy personnel. The SIGINT unit monitored enemy communications to determine future enemy movements and intentions. Finally, the HQ unit supervised the activities of the other three sections and kept them adequately supplied so each unit could perform its job effectively without interruption. With the exception of the UAV unit, most of the missions were team-based; hence, the cost of not being able to field an additional team was not complete mission failure. Fewer teams simply meant that the MICO could not perform HUMINT or SIGINT services in as many geographic areas for the BCT. This observation represented a critical turning point for the future training and employment of the MICO.

I then carefully managed the expectations of my higher headquarters by explaining to officials there that, with the amount of personnel and equipment on hand, the MICO could still perform its wartime mission. It just could not provide intelligence support to as many different battalions as the brigade leadership originally wanted. My superiors understood the difficult situation facing the MICO and appreciated my honest assessment of what the company could actually do. I then established a glidepath for the level of proficiency the MICO needed to achieve to provide the level of intelligence coverage necessary for Afghanistan. I also created intermediate benchmarks that charted company progress over the next few months to ensure we were on track to achieving our proficiency goal. Around this time, the Army came online and created a 4-month fielding and training program for the UAV unit beginning in August. This allowed me to focus the majority of my efforts on developing the HUMINT, SIGINT, and HQ units.

First, I leveraged the collective experience of the intelligence personnel in the 82nd Airborne Division Analysis and Control Element (ACE) and several intelligence-specific Mobile Training Teams (MTTs) to help the SIGINT and HUMINT soldiers gain experience in performing their wartime mission. Additionally, with the help of my 1SG, each section developed a reception and integration system that immediately integrated any new personnel into the unit and in a truncated period of time provided them with all of the intelligence-specific training they had missed prior to their arrival. Every few weeks, as additional people and equipment started to trickle in, I examined where the company stood in relation to each benchmark and how close or far we were from the glidepath. Even as small portions of the company deployed with the brigade advance party or early main body, the remainder of the MICO personnel continued to train until they deployed.

As a result of understanding the mission that my company needed to perform in combat, leveraging the collective experience of my subordinates and other senior intelligence professionals, establishing benchmarks, continuously monitoring training progress, and tireless devotion, I survived my crucible experience. When the time to deploy did arrive, the MICO possessed 90% of its required personnel, trained and ready to deploy with all of their required equipment. The Company performed superbly in Afghanistan and sustained no combat fatalities.

My crucible experience will undoubtedly prove invaluable throughout my life. I know that, whatever position of increased responsibility I assume following ILE, I will feel at least slightly unprepared. However, I am certain the confidence I gained from my crucible experience will assist me as an organizational leader because I learned to overcome significant managerial challenges and succeed in a complex and dynamic environment despite little help or guidance from my higher headquarters. I realized I can operate primarily on commander's intent, utilizing sound judgment, and leveraging the collective experience of others, whether subordinate, superior, or outside the immediate organization, to achieve the desired endstate. I also better understand the significance of realistic, battle-focused training, providing subordinates with clear guidance and intent, and subordinate leader development. I will impart this newfound understanding on the subordinate leaders within my future organization to better prepare them for their own crucible experiences.

The following are my recommendations to other division-level and below military officers to reduce the strain on today's young military leaders. The current high operational tempo for tactical units will likely continue for the next five years, even with the proposed troop draw-downs in Iraq and Afghanistan. This means that young and inexperienced officers will continue to occupy key intelligence positions prior to receiving all of the training and experience necessary to ensure their success. Therefore, at the Brigade Combat Team level, BCT S2s must work closely with the Commander of the STB to ensure they identify the most competent and qualified captain to serve as the Commander of the MICO. This may require recruiting outside the parent BCT to find the right person for the position. Additionally, the Brigade Commander should make every attempt to ensure one of the top three leaders in the STB is an MI officer. This provides additional oversight for the inexperienced MI Company Commander and further ensures the company is appropriately trained and correctly employed in a tactical environment.

At the division level, the G2 must work closely with the Division Commander and each BCT Commander to ensure one of the top three leaders in the STB is an MI officer, unless the Division Commander and BCT Commander consciously choose otherwise. Additionally, since the MICO consists of four different sections, each requiring individual low-density training that the MICO or the STB alone cannot provide, the Division G2 should work with the ACE Chief and installation MI-specific training personnel to ensure that each BCT MICO is receiving the appropriate low-density training, as the Division ACE and other MI-specific MTTs are much better suited to provide this "INT"-specific training than the STB or the BCT. Obviously, if the Division G2 provides this level of oversight, significant opportunity for micromanagement and conflicts exists between Division and Brigade. Only well-developed personal relationships among the Division G2, the BCT Commander, the BCT S2, and the STB Commander can create and maintain the necessary balance between establishing a trained and ready MICO vice placing the MI Company Commander under significant scrutiny from four different bosses.

Finally, at the Army Intelligence School and at installation-level MI training centers, intelligence personnel and contractors must take a proactive approach when interacting with young intelligence officers. Many MI officers straight out of the schoolhouse or transition course suffer from a lack of knowledge about what intelligence assets exist, what training programs are available, and whom to contact to take advantage of these opportunities. When briefing captains at the MI Career Course or new lieutenants at the MI Officer Basic Course, briefers should always provide these officers with point of contact information to ensure that the knowledge provided extends well beyond a 30- or 60-minute PowerPoint presentation and that reach-back capability is always present. We cannot prepare MI Company Commanders and their units for every potential challenging situation that might arise. However, implementing the previously mentioned suggestions ensures that each deploying BCT deploys with an appropriately trained and properly prepared MICO, capable of overcoming adversity when it strikes and providing the BCT with the timely and accurate intelligence that it needs.

MAJ Joe Kosek is a recent graduate of the U.S. Army Command and General Staff College (CGSC) and is beginning his tenure as Brigade S2 for the 3rd Brigade Combat Team, 4th Infantry Division, at Fort Carson, CO. He began his career in Armor and served as a Tank Platoon Leader, Scout Platoon Leader, and Headquarters Troop Executive Officer in Korea. In 2005 he transitioned to MI and served at as an Infantry Battalion S2, a tactical Military Intelligence Company Commander, and a Reconnaissance, Surveillance, and Target Acquisition (RSTA) Squadron S2 at Fort Bragg and in Afghanistan. He

also served as an Assistant Professor of Military Science at the University of Notre Dame for two years prior to attending CGSC. MAJ Kosek holds a BBA and MBA from Notre Dame and an MA in Security Studies from Kansas State University. He has been awarded the Bronze Star and two Meritorious Service Medals.

[Editor's Note: At the time he submitted this essay, the author was a student in ILE Class 11-01. For those old-school readers like myself unaware of the recent transition from the long-standing CGSC resident and non-resident system terminology, "Intermediate-Level Education refers to the third tier of the Officer Education System and is directly linked to Army Transformation." According to its mission statement, ILE will prepare "field grade officers with a warrior ethos and warfighting focus of leadership in Army, joint, multinational, and interagency organizations conducting full spectrum operations."]

Notes

[1] Bennis, Warren G., and Thomas, Robert J., "Crucibles of Leadership," *Harvard Business Review* (2002), 2.

Markus Wolf:
One of History's Most Effective Intelligence Chiefs

by Dr. Kenneth J. Campbell

INTRODUCTION

This article seeks to explain why Marcus Wolf was such a successful espionage chief, which can be useful to those who select future chiefs of military intelligence. The first part of this article is a review of Wolf's background. The second part considers his achievements under the following headings: use of "Romeo" spies; penetration of the German government; utilization of disinformation; his doubling of the CIA's agents; and the acquisition of the "Crown Jewels." In the last part I will attempt to clarify the traits which made Wolf so successful, i.e., the background qualities that enabled him to produce so brilliantly. Unfortunately, Marcus Wolf was not one of our own intelligence leaders, but we can still learn from his life and work, no matter how odious some of his methods may have been.

BACKGROUND

Markus Wolf was born in Baden-Wuerttemberg, Germany, on 19 January 1923, the son of a Jewish doctor, writer, and communist activist. He spent his first ten years in Stuttgart, but when the Nazis came to power they made life intolerable for the Wolf family. His mother and the children were smuggled into Switzerland with the help of communists and later to France. When the Nazis had seized all of their property, the parents accepted asylum offered by the Soviet Union, at a time when Markus was only eleven years old.

In the Soviet Union, Markus Wolf's world view was formed when he entered the Karl Liebknecht School for children of German-speaking parents in 1938,[1] although he completed his secondary education in a Russian high school in Moscow. Markus and his brother, Koni, joined the Soviet Young Pioneers, an organization similar to the Boy Scouts, and marched in Red Square in front of Soviet dictator Josef Stalin. This was the time of the purges of 1936-38, when many of his teachers disappeared, and in order to get out of the USSR his father volunteered for service in the Spanish Civil War, fighting against General Francisco Franco's Nationalist forces.

Upon graduation from high school, Marcus was admitted to the Institute for Aircraft Construction, but his dream of building planes was shattered by the German invasion of the Soviet Union on 22 June 1941. As the German Army approached Moscow in the summer of 1941, the families of the Writers' Union, a privileged group, were evacuated to Kazakhstan. Suddenly in 1943 a telegram arrived from the Executive Committee of the Comintern ordering Markus to go to Ufa, capital of the republic of Bashkiria, and then to Kuschnarenkovo,[2] 40 miles from Ufa, to attend a Comintern training school, where he learned intelligence methods along with the use of firearms before his return to Germany. Markus's father, Friedrich, had already been ordered to return to Moscow to be part of the administration of the Red Army, where he took his wife and son, Konrad.[3] Students at the Comintern school were taught covert methods—"how to use submachineguns, rifles, and pistols; how to handle explosives and hand grenades; and how to use "conspiratorial techniques" of meeting and message passing…"[4] They were also taught the methods of producing propaganda. At this time Markus met his future first wife, Emmi Stenzer, to whom he remained married for 30 years before divorcing her. The dissolution of the Comintern occurred in May 1943 to mollify the British and American leaders, who were angry about the subversive activities of its agents.

After Wolf's examination in this school, GRU (Soviet military intelligence) official Anton Ackermann persuaded General Sergeij Schtemenko to send Wolf to Moscow as an editor and radio commentator on the *Deutsche Volkssender* (German People's Radio), a propaganda unit. General Schtemenko, a GRU chief, recognized Wolf's potential.[5] Wolf succeeded in this job, which Ackermann reported to the general. Later Ackermann recommended that Wolf head the future German intelligence element, but only after he had "learned the ropes" of this task. This period was designed to be long enough so as not to excite the anger of older men who had been in intelligence for a considerable period of time.

In late May 1945, Wolf, now 23 years old, returned to Germany and assumed a position at the Soviet-controlled *Berliner Rundfunk*. He stated at that time that Germany was still his *Heimat* (land of his birth), and he was appalled at its destruction, but he wanted to purge Germans of their dedication to Nazism. In a letter to his parents he described the Soviet troops as without a word of hatred for the Germans,[6] much in contrast to the reality of their rape and pillage against the German population described by such authors as Norman M. Naimark.[7] For Markus, socialism was a liberating force, since it had rescued him from Hitler, and he believed it could only produce a new man, incapable of the terrible violence going on around him.[8] This was the beginning of his self-confessed filtering of Soviet crimes from his mind, the psychological defense of a young man desperately determined that communists could only do redemptive work.

Beginning in September 1945, Wolf covered the Nuremberg Trials for the radio station as a special correspondent under the pseudonym of Michael Storm, the success of which earned him a career in diplomacy with the founding of the German Democratic Republic (GDR) in October 1949. On 1 November 1949, he was sent back to Moscow as part of the new East German diplomatic mission there, requiring him to give up the Soviet citizenship that he cherished. The ease of this life was pleasant for Marcus and his wife, Emmi. While in this position, he met Stalin and saw Mao, referring to both of them as "monuments of history" instead of the mass murderers that they were, indicative of his ability to filter out reality.[9]

In 1951 he was sent back to East Berlin, the Soviets having assigned him to the newly created *Aussenpolitischer Nachrichtendienst* (APN), an intelligence facility disguised as the Institute for Economic Research, where he started on 16 August 1951. His rise through the ranks of this organization was rapid. For a while he was guided by the Soviet Anderi Grauer, who later collapsed under the pressure of his intelligence career and descended into paranoid schizophrenia. Other Soviet "advisors" succeeded Grauer, also keeping a firm hand on East German espionage. Markus was helped in his new work by German mentors, such as Horst Jaenicke, 19 years his senior, and Richard Stahlmann, 32 years older than himself.[10]

On 1 December 1952 Walter Ulbricht, the head of the GDR, promoted Wolf to head the APN of the *Ministerium fuer Staatssicherheit*, MfS or Stasi, despite the fact that Wolf was not yet 30 years old and had only 16 months of experience in intelligence. Wolf took over the APN from Anton Ackermann, who had been his prior mentor when Wolf was quite young. In 1956 Ernst Wollweber, an accomplished saboteur of ships, was head of MfS. That year Wollweber reorganized the GDR security system due to the alleged failure of the MfS to control the worker's revolt of 1953.[11] In this process Wollweber changed the name of Wolf's APN to the *Hauptverwaltung Aufklaerung* (the Main Administration for Intelligence, or HVA), the foreign intelligence agency, whereas the MfS concentrated on domestic control. Wolf was promoted to Major General six months later.

In 1957 Erich Mielke was able to replace Wollweber as chief of the MfS. Wolf's tenure as head of the HVA, always under Mielke, sometimes reflected a supportive relationship and other times one of stormy rivalry, since Mielke over the years sought to replace Wolf.[12] Mielke, according to Wolf, wanted to put a "brake" on his career, whereas Wolf wanted to be independent.[13] The HVA was run chiefly by Soviet advisors until approximately 1960, a time when Wolf, still a newcomer to intelligence, had learned his job through on-the-job training for eight years.

Wolf's admiration for Stalin, somewhat surprising since he had seen the purges of 1936-38, was strong, a feeling which ran deep into his childhood. The speech of Nikita Khrushchev at the 20th Congress of the Communist Party in February 1956 shook Wolf and millions of other communists, as Khrushchev described the terrible crimes of Stalin, one of the most bloody dictators of the 20th century.[14] Still, despite the failings of the socialist system, Wolf considered it to be a superior model to that of the West, focusing on how far communism had brought the backward societies of Russia and China. In discussing the lives of George Blake and Kim Philby, British traitors to the West, Wolf seemed to describe his and their dedication to the secular religion of communism.[15]

If you have conviction in life, you follow the road you have set for yourself and do not deviate from it—no matter what terrible things you see along the way.[16] In the 1950s, East Germany was in turmoil as thousands of its citizens fled to West Berlin and then to West Germany, depriving the GDR of some of its best educated and most capable people. It is not generally stressed in the West, but during this period thousands of British, American, and French spies swarmed into East Germany. The East German government, armed forces, factories, and research laboratories were deeply penetrated by spies, a position from which Western intelligence agencies could operate against the rest of the Soviet Bloc. Both the U.S. intelligence services and the German BND (*Bundesnachrichdtendienst*) engaged in mass espionage in the GDR.[17]

At the same time, Wolf sent young and politically motivated men into West Germany who provided the basis for his later long-term agents, his main successes.[18] The HVA sent among the refugees its own agents, and the

number of refugees was so great that Western security services could not identify many of the East German intelligence officers. Since the two Germany's shared a common language and culture, these agents were able to infiltrate their target with ease. The universities[19] were an especially tempting target, since a student could be recruited and later guided into a research institute after his doctorate was completed. Surprisingly, when the *Rosenholz* files were examined, very few professors were part of the HVA web of espionage in this target country.[20] Wolf also set up rooms in East Berlin, complete with prostitutes and cameras hidden in the bedroom, a project designed to blackmail West Germans into working for East Germany.

The MfS installed an Office for Technology and an Office for Atomic Research in 1956 to evaluate material stolen from the West and then to direct this information to various scientists and industry. Care was taken to mask the material so that its source in West Germany could not be traced by Western intelligence. By 1989 the number of evaluators engaged in this task had increased from 35 to approximately 500, suggesting considerable success in the collection of scientific and technical intelligence to require so many scientists and other personnel to scrutinize incoming material.[21] At approximately this time, several East German HVA officers acquired blueprints for West Germany's "Leopard 2" tank and the fighter plane "Tornado,, spectacular evidence of HVA successes. The Soviets could have used this information to defeat West German tanks and planes in the event of war. During the period 1972 to 1989, the evaluators received 21,000 pieces of information, nearly half of which came from Washington, DC[22] Much of this material was acquired through attendance at conferences and often originated in the Silicon Valley, an American center of research.

Finally, Kruschchev and Walter Ulbricht, the East German dictator, decided to close the East German border in August 1961 by constructing the infamous Berlin Wall. Although Wolf claimed that the construction of the Wall came as a surprise to himself, it is unlikely in view of his position in the East German Politburo.[23] This raises the question of why Wolf would need to fabricate such a story. Another question is why Wolf does not mention Western espionage in the GDR as a factor in the decision to build the Wall.

Wolf also concentrated on meeting West German industrial contacts who were anxious to do business in the GDR. For example, at this time he met Christian Steinruecke, involved in wholesale and steel trading in West Germany, a contact which lasted many years, and he was able to penetrate the Krupp empire through Carl Hundhausen, a member of the board of that firm.

Wolf found much of intelligence boring, requiring him to sift through vast amounts of information to find occasionally something worthwhile, varying this routine by running 10-12 agents personally and meeting them in safe houses in East Berlin.[24] He often discussed philosophy with them—the meaning of life and one's dedication to something higher than themselves. This procedure also gave Markus Wolf a "close-up" view of the problems encountered by his own intelligence officers so that he understood their concerns more clearly and could thus gain their allegiance. Consequently, only one major defection, that of Werner Stiller, occurred during his 34 years as chief of the APN and HVA.

THE WOLF AND HIS ROMEOS

Whereas espionage in the past involved erotic women prying military and state secrets from their lovers, Markus Wolf reversed the situation in using men to gain secrets through women.[25] Wolf saw an opportunity and seized this possibility in a remarkably creative way, when he took control of the HVA in approximately 1960. In postwar West Germany, there was a shortage of men, as four or five million young Germans had been killed during the war. As a result, many young women had to give up hope of marriage and children, instead concentrating on their careers as secretaries and administrative assistants, where they eventually worked for men of considerable positions in the West German government or business. Wolf therefore sent attractive but manipulative men, his "Romeos," after these vulnerable women to obtain West German secrets.[26]

The woman selected for pursuit by a "Romeo" was not selected at random, but the Stasi would have done a personality profile on her to see if she were a likely candidate for this relationship.[27] If she were, suddenly a "Romeo" would appear in the life of this middle-aged woman and, after beginning a relationship with her, he would explain that he needed a copy of an innocuous document for the research he was performing for his job in one of the institutes or for his dissertation. Perhaps the couple would decide to get married and at that time the importance of the documents that he claimed to need would increase, until she was engaged in espionage along with her husband. As Wolf himself remarked, many of the women were unwilling to admit to themselves for a long time that they were working for the HVA,[28] and he also stated, perhaps defensively, that no woman could be forced into espionage against her will.[29] Upon confrontation with German counterintelligence, this woman would ask for her husband, only to be told that her "husband" was really not her husband, since they had been "married" by a KGB fake priest and witnessed by KGB fake in-laws. She would then be told the crushing fact that her "husband" had already

absconded to East Berlin via Belgium, Holland, or Switzerland. In one case this realization resulted in a suicide. These women were usually sentenced to prison, the length depending on the estimated amount of damage their espionage had done to West Germany.

However, as West German counterintelligence began to look for single men travelers between the ages of 25 and 45 with a small amount of luggage and a certain type of haircut, these targets were tailed by undercover men and often apprehended. This gradually meant that Wolf's use of Romeos had to be curtailed. As yet, we do not, and may never, know how much useful intelligence was obtained through the use of the "Romeo" method of espionage. We do know that some of the women implicated in this espionage delivered documents to the HVA for years before they were arrested. However, Wolf and the leaders of the HVA did appreciate the results of this method of espionage. Two of the leaders involved in this kind of activity, Colonels Rudolf Genshow and Otto Wendel, were awarded the degree of Doctor of Jurisprudence, *Magna cum Laude*, from the Stasi Hochschule in Potsdam for their work in this program.[30]

The most damaging example of a senior-level employee in the BND spying for the HVA was the case of Gabriele Gast, who began as a doctoral student doing her dissertation in Karl Marx Stadt on the political role of women in the GDR. There she met an MfS major, Karl Heinz Schneider, with whom she fell deeply in love, attracted to the proletarian charm of this man. Schneider, who "offered to help her with her research,"[31] gradually manipulated her into a very close relationship. When asked to cooperate with the East Germans, she hesitated until being told that, if she refused, she would never see Schneider again. Being horribly naïve, she agreed to spy for the HVA. She was provided with the latest methods of communication, an improvement over the use of invisible ink. This included the transfer method which allowed her to send innocuous messages along with the intelligence which she was transmitting.[32] Her doctoral supervisor, Professor Doctor Klaus Mehnert, who had contacts with the BND, strongly recommended her for a position as a political analyst in this organization, which, when she obtained it, delighted Markus Wolf.[33] She gave the HVA an "accurate picture" of the West's knowledge and assessments of the Soviet Bloc's military power, which enabled her to meet her lover in East Germany on holidays, despite BND prohibitions against such excursions.

Wolf, very much aware of Gast's importance, personally met her and Schneider in such places as Yugoslavia, where he formed a close bond with her. She had the feeling of belonging, something she evidently missed in West Germany. In this relationship she was enabled to mix idealism with personal commitment, something Wolf believed was the mixture which enabled people from an upper-middle class background and "complex personalities" to "flock" to his service.[34] Eventually she was able to become deputy chief of the BND's political department of the Soviet Bloc, a position from which she could give the HVA invaluable information before her arrest in 1990 and subsequent imprisonment. In this position she met and exchanged information with CIA officials in Washington and British MI6 leaders in London, finally gaining access to every bit of information available to the BND. One of her jobs with the BND was to prepare a highly classified report for Chancellor Helmut Kohl."[35] In 1989 the East German government collapsed, and afterward Colonel Karl-Christoph Grossmann,[36] seeking to save his own hide, went over to the West and gave information which pointed only to Gaby Gast.

PENETRATION OF THE WEST GERMAN GOVERNMENT

Marcus Wolf sent his officers into every significant part of the West German government and society in the effort to guide their moves into the political parties, government, universities and high schools, and peace movements.

At one time Wolf had approximately 120 *Inoffizielle Mitarbeiter*[37] in West German political parties and eight members of Parliament in his service.[38] Some of his most significant agents who influenced the Bundestag are described below.

One of his prize agents was Josef Braun (1907-1966) who joined the Communist Party in 1927, fought in World War II, and then spent time in an American POW camp. He received orders in 1952 from the *Aussenpolitischer Nachrichtendienst*, the forerunner of the HVA, to join the SPD (non-Communist Social Democratic Party or Socialist).[39] HVA Chief Wolf supervised his work under the code name "Freddy" and called Braun "a source of incalculable value."[40] Wolf and Braun were friends who discussed politics, philosophy, and life.[41] Braun relayed information about developments at the top of the SPD to Wolf and as an agent of influence guided policy decisions favorable to the GDR (German Democratic Republic, or Deutsche Demokratische Republik).[42] He was rewarded with roughly 300 DM (Deutsche Mark) each month.[43]

Another of Wolf's agents with strong influence in the West German government was Hans-Adolf Kanter (1925-), whose long friendship with Helmut Kohl was helpful in his political and intelligence career. When Kohl was elected Chancellor in 1982, Kanter was able to gain access to important government documents, sending 1,200 reports to

the HVA.[44] Further, Kanter rented a house to Egon Bahr, an SPD politician who used this building in mapping out the negotiating positions of the West German government toward the GDR. This enabled the HVA to bug the house and for the East German government to have an advantage in these negotiations.[45]

The Free Democratic Party (FDP) was a right-wing, pro-business group to which Markus Wolf turned his attention. Wolf persuaded Hannsheinz Porst, who owned a nationwide photography business, to join the FDP, an organization in which he provided Wolf information about this party. In 1969 Porst was convicted of espionage and sentenced to two years and nine months in prison.

William Borm, a member of the *Bundestag*, was recruited by the HVA, oddly enough after his release from a GDR prison, and joined the FDP. He was elected to the *Bundestag* in 1965 and the European Parliament in 1971, both important positions from which he could support measures favorable to the GDR. From 1969, Wolf directed Borm to influence the FDP's opposition to pro-American Chancellor Conrad Adenauer's rearmament and its insistence on the pressing need for an understanding between the two German states.[46] Wolf even wrote the outline "of a speech delivered by Borm to the Bundestag in October of that year."[47] Borm, a leader of the FDP, was very distrustful of NATO and endorsed the German peace movement which Wolf supported with other agents and funds. Instead of going to jail, Borm received an honorary doctorate from the University of Leipzig in 1987.

Wolf's relationship to Herbert Wehner, an SPD politician and communist in his youth, was mixed. On one hand, he considered Wehner to be a traitor to his associates from his early period,[48] since Wehner had informed to Swedish authorities against them. He also considered Wehner to be an agent of influence, but not an agent in the classical sense. An agent of influence is someone who uses "his or her position, influence, power and credibility to promote the objectives of a foreign power…"[49] Certainly this is an indictment of Wehner in terms of his service to the West German government. Above all, Wolf's feelings toward Wehner were mixed, mirroring Wehner's conflicted relationship to the GDR.

Willy Brandt's election to the Chancellorship in 1969 brought new opportunities for Wolf to penetrate the West German government. Above all, he had an agent in Brandt's office, Guenter Guillaume, who, after Brandt's reelection in 1972, became one of the Chancellor's aides. Brandt pursued *Ostpolitik*, détente toward the Eastern Bloc, which promised to reduce tensions in East and Central Europe. It was a good time for Wolf, since "an agent" in Brandt's office sent him the first draft of Brandt's speeches.[50] Guillaume sent information to Wolf through two couriers, whose identities are still unknown, and some of this information concerned President Richard Nixon's views on nuclear strategy.[51] Guillaume also informed the HVA about Brandt's private live, and his numerous liaisons with various women, but this was never used as a means to blackmail Brandt. As the result of Guillame's exposure as a spy and arrest in 1974, Brandt shortly afterward had to resign as Chancellor. Wolf stated that the worst defeat his HVA suffered was Brandt's fall, failing to consider that his placement of a spy in Chancellor Brandt's office was his greatest success.[52]

Karl Wienand was an SPD staff member in Parliament, and at the same time an agent of influence for the HVA. Wienand had close contacts with Herbert Wehner and Helmut Schmidt, who later became an SPD Chancellor.[53] Wienand sent the names of people under suspicion of espionage to the HVA, enabling the HVA to decrease its activities until they were no longer the target of investigation.[54] He was arrested and convicted of espionage in 1996 and sentenced to two and a half years in prison, being pardoned by President Roman Herzog in 1999 because of his health problems.

Klaus Kuron was an employee of the *Bundesamt fuer Verfassungsschutz* (BfV, the German counterintelligence agency). He recognized that his career was going nowhere for lack of a university degree, but he also needed more money in order to educate his sons. In September 1981 he contacted the HVA to begin another occupation—that of treason. He justified his betrayal by telling himself that the less advantaged in West Germany find roadblocks in their way, as he was experiencing, and the lazy sons of the rich are protected.[55] Once the German Democratic Republic collapsed in 1989, Kuron's first handler, Colonel Karl-Christoph Grossmann, reported him to West German counterintelligence officials.[56] Although he was given the opportunity to relocate to the Soviet Union, Kuron chose to stay in West Germany and face prosecution. He was convicted in 1992 and sentenced to twelve years in prison, but served only eight years of his term.

Hansjoachim Tiedge was in a senior post in the BfV, dealing with espionage in the German Democratic Republic, a post from which he could report the names of many West German agents working in East Germany. His "personal problems—alcoholism, gambling debts, and the accidental death of his wife—reached such a point that the only alternative, in his mind, was to defect to the HVA."[57] He was no communist, but as a security risk his days with the HfV were probably numbered. Needing to prove his worth to his new controllers, Tiedge believed he was revealing damaging information to the HVA, not realizing that Kuron already had been working for Wolf and had

already revealed basically the same material.[58] Once Tiedge defected, the HVA worked to restore his mental and physical health, whereupon he wrote a dissertation at Humboldt University in East Berlin on the BfV counterintelligence methodology, for which he received a doctorate in law. Upon the fall of the GDR, he went to Russia, where he and his new wife lived under a new identity.

DISINFORMATION

This type of espionage can be defined as the attempt to influence the decision- makers and most thoughtful people of the enemy nation in ways which disrupt the foreign and defense policies of that government. This is usually accomplished through the attempt to influence "opinion makers"—members of parliament, the faculties of universities and schools, and the most active and well-educated segments of that society.[59] Disinformation, along with propaganda, assassination, and other delicacies, may be lumped together under active measures, which in East Germany were strongly influenced by the model of the British Sefton Delmers, one of the leaders in propaganda against the Germans in World War II.[60] The HVA could also count on the Swedish Communist Party and leftist organizations of that nation to distribute its propaganda.

In East Germany the original leader of active measures was Albert Norden, a rabbi's son who "went wrong" and became a member of the East German Politburo, where he served in this capacity until his death in June 1982.[61] His strategy was to expose the former Nazis in positions of power or influence in West Germany, presenting the GDR as anti-military, the guardian of peace. When the MfS continued this tradition after Norden's death, Markus Wolf saw the prestige of the HVA threatened by the MfS and began to employ its technique, chiefly disinformation, beginning around 1966. Wolf also acted to increase these measures according to orders from Moscow, and established Department X under the leadership of Colonel Rolf Wagenbreth, who led this unit until 1989 when the GDR collapsed.[62] The methods of the HVA were not controlled by a parliamentary committee and so were based on the Machiavellian philosophy of the ends justifying the means, as explained by two of its former analysts.[63]

In 1970 Wolf had a press conference at which eight West German physicists accused the West German government of working to develop atomic weapons, a very serious charge in West Germany at that time.[64] This was nonsense, but to the Germans in both nations, who had become horrified of war through the trauma of two World Wars, the accusation was a powerful, though nonexistent, threat.

In March 1971 Markus Wolf stressed that the HVA should penetrate groups of students, writers, and other groups, especially students who concentrated in law, journalism, the natural sciences, and their organizations.[65] Wolf even advocated working with university and high school students[66] in the GDR. The HVA repeatedly made contact with individual journalists in West Germany rather than attempting to set up its own press there, helping West German journalists in their research on topics concerning the GDR and attempting to discredit intelligence organizations of Western nations as pioneers of the Cold War.[67] This continued, as reality was pushed aside by the HVA through spreading nonsense and rumors.[68]

Wolf knew that the concept of peace was very persuasive to a nation traumatized by war, citing the power of peace movements in Westerm Europe in a speech in January 1982 and urging socialist nations to broaden and deepen their influence in NATO countries through political parties and churches. His HVA was instrumental in the formation of a group of retired NATO generals and admirals from Norway, Portugal, England, Greece, Italy, France, the Netherlands, and West Germany in an effort to support peace groups. The HVA, in close cooperation with the KGB, provided these military leaders with a large number of background papers and relevant documents. This effort was organized by Lieutenant Colonel Manfred Laszak, head of Subdepartment II in Department X of the HVA.[69]

RENDERING THE CIA INEFFECTIVE IN EAST GERMANY

In the 1980s the HVA and MfS rendered the CIA "deaf, dumb, and blind"[70] in East Germany by the utilization of double agents. These double agents pretended to spy for the CIA, but instead served the HVA or agents of the MfS. This assertion is supported by the former Deputy Director of Central Intelligence, Admiral Bobby Ray Inman; former CIA Director and Secretary of Defense Robert M. Gates; and Milton Bearden, "the last chief of the CIA's Soviet-East European Division."[71] The CIA has consequently tried to cover up these terrible defeats and national security lapses. By recruiting American servicemen in signals intelligence, the HVA severely disabled U.S. electronic intelligence and, in the process, U.S. national security.

The CIA was consequently deprived of accurate intelligence so that when the East German people revolted against their government in 1989, the CIA seemed surprised. The same occurred when the Berlin Wall came down that same year.[72] In contrast to the incompetence of the CIA, the HVA "saturated" West Germany with agents, who compromised West German government officials and recruited NATO personnel, especially those engaged in signals intelligence. One estimate indicates that East

German intelligence recruited roughly 17,000 to 23,000 agents in West Germany.[73] "Five out of every 100,000 West German citizens spied for East German intelligence…," according to Dr. Benjamin B. Fischer, former Chief Historian of the CIA. Wolf stressed the recruitment of moles in Western intelligence, people who provided him with daily reports in reference to investigations and surveillance, thus making Western defenses far less reliable. These moles were CIA officers,[74] American servicemen, businessmen, and students in West Germany.[75]

Two former HVA officers, Klaus Eichner and Dr. Andreas Dobbert, published a book, *Headquarters Germany*,[76] whose title is in English, but the text is in German. The extent of the HVA's penetration of the CIA was clearly exposed, a frightening document in view of the vulnerabilities of the Agency. This book covered such topics as the history of the CIA and its entire structure; its relations with the Gehlen (BND) organization; the military and diplomatic offices which served as CIA cover in Bonn, West Berlin, Frankfurt/Main, Hamburg, Munich, Stuttgart, and Cologne; the names and tenure of its chiefs of station in Bonn, West Berlin, and the DDR; the locations of various CIA offices in West Germany; the telephone numbers of some of these offices; the organizational changes within the CIA in Europe; the number of employees which Ted Shackley had in West Berlin; where different CIA officers had been stationed in various parts of their careers; the names of the *omas* in different CIA homes; the names of dissatisfied CIA wives; which CIA officer had a glass eye and the fact that he played tennis; CIA officers who had cooperated with the HVA or MfS; the arrests of CIA officers in the Soviet Union; CIA attempts to suborn diplomatic personnel in foreign countries; how Edward Lee Howard's information led to arrests in East Germany; activities of the Counter Intelligence Corps; the work of the Aspen Institute in West Berlin; the structure and objectives of the U.S Army's Intelligence and Security Command (INSCOM); and many more aspects of U.S. intelligence. There is no question—Markus Wolf and his HVA thoroughly penetrated the CIA in Europe.

THE CROWN JEWELS

An even more damaging HVA penetration occurred when Sergeant James W. Hall of the U.S. Army, a specialist in SIGINT (signals intelligence) operations, passed on critical intelligence, the so-called CROWN JEWELS, to HVA officers. Hall had been working on an operation that sought to provide NATO authorities with early warning of an impending attack by Warsaw Pact forces and plans for a destructive counterattack.[77] Hall's motivation was relatively simple—he was greedy and felt that he needed more money for his family and various hobbies. Hall worked in the NSA's Field Station Berlin (FSB), America's main SIGINT site located on top of a pile of rubble in West Berlin, often referred to as Teufelsberg (Devil's Hill). From here the U.S. and Great Britain could eavesdrop on Warsaw Pact forces as far as 300 miles deep into enemy territory.[78] A staff of 1,300 Americans, not including the British, targeted Warsaw Pact "command-and-control centers and field communications, troop movements, maneuvers, and strategic exercises," which could warn NATO leaders of a possible enemy attack.[79] Hall's intelligence to the HVA included a study of how the Americans could jam the Soviet General Staff's command and control system, which was to be utilized to issue orders to "…its strategic missile forces and missile-carrying submarines…"[80] The HVA officers who received Hall's material, such as Klaus Eichner, said that it gave them "goose-bumps," which is very understandable, since it probably would have enabled a Soviet victory over the Allies in the event of war in Europe.[81] The Soviets were consequently able to install scrambling devices to defeat these potential NATO measures.[82]

Another important HVA agent was an Air Force enlisted man, Jeffrey Carney, who was born in Cincinnati, Ohio, and was sent to West Berlin at the age of 19. Confused about his sexuality and having engaged in at least one homosexual relationship, he was vulnerable to HVA handlers whom he began to see as his friends. Carney passed roughly "sixty-five pieces of information" to the East Germans between 1983 and 1986, material concerning his unit's electronic activities against East Germany and the Soviet Union.[83] This activity was directed by the NSA to its West Berlin stations. Carney's documents indicated that the United States had conceived of a plan to intercept Soviet ground-to-air commands, while substituting their own orders through collection of the voices of Soviet commanders.[84] U.S. servicemen and women in West Berlin were an easy target for the HVA due to their relatively low pay and the moral chaos in which they were raised in the United States, suggesting that more of them have sold secrets to the enemy but have not yet been caught.

Although the HVA destroyed most of its files after the fall of the Berlin Wall in 1989, the CIA did obtain copies of the names, addresses, and workplaces of most of its agents and backup staff, another version of the CROWN JEWELS on index cards. Almost one-half of these agents belonged to the HVA's unit for scientific-technical intelligence gathering, the *Sektor fuer wissenschaftliche-teknische Aufklaerung* (SWT) (Sector for Science and Technology Intelligence),[85] although Western companies had no interest in admitting that some of their employees were spies. The SWT had agents planted at prestigious firms in West Germany, such as IBM, Siemens, Texas Instruments,

DEC,[86] and AEG/Telefunken, a producer of electrical equipment. The large number of these agents at various Siemens companies in West Germany is striking.[87]

When President George H.W. Bush saw the looting of the Stasi headquarters on TV, he asked the CIA to obtain some of the documents, spurring on Director of Central Intelligence William Webster to push his organization, the CIA, into action. The first "tranch" of this material was obtained in January 1990, when an HVA counterintelligence officer, Rainer Wiegand, sold some of this material to the CIA, revealing that every one of the CIA's recent agents in East Germany had been doubled.[88] Other files had been flown to Moscow, where the CIA obtained them for one million dollars[89] from an unhappy KGB officer, the details of which we as yet do not have. These files are referred to as *Rosenholz* (Rosewood) and were sent to CIA Headquarters in Langley, Virginia, where they listed thousands of HVA agents operating in the West. This material can allow Western scholars in the future to determine who these agents were, why they spied, and other details of their tradecraft, though researchers as yet do not have access to these files. In the early 1970s the HVA had begun to microfilm the material on its agents, a process facilitated in the 1980s when the fear of a nuclear war seemed real to the leadership of the HVA. During this period, President Ronald Reagan baited the Soviet Union into an arms race in order to break it economically. When the CIA revealed some of this material to the West German government, it resulted in the arrest of many former agents, resulting in 257 convictions.[90]

The motivation for this spying was evenly split between greed and ideology, the latter represented by idealistic people seeking to promote world peace and to establish all of Germany as a socialist state.[91] As a whole, it is likely that 6,000 West Germans and 20,000 East Germans spied for the HVA, an astounding achievement by Markus Wolf.[92]

HVA techniques were such that it was very difficult for West Germany to penetrate their webs. Their agents were equipped with the necessary communications technology—secret writing, shortwave radios, codes, microdots, and dead letter drops.[93] Case officers were not permitted to "recruit or handle agents in West Germany," which demanded new types of intelligence personnel—the recruiter and the instructor. The recruiter's task was to identify likely agents and to enlist them in espionage, whereas the instructor trained the agent, passed on instructions from the HVA, and met him in a third country, like Austria, Italy, or Yugoslavia. The instructors, all East Germans, often brought back the agent's material to East Germany. All HVA material was passed on to the Soviet Union, which meant that the intelligence war between the West and the East was probably won by the latter.

THE FINAL YEARS

On 15 November 1986, Markus Wolf retired from the HVA, which then numbered about 91,000 employees.[94] Although there are conflicting statements as to the reasons for his retirement, Wolf's explanation is interesting in that he claims he felt trapped within the stagnated bureaucratic system within which he worked.[95] On the other hand, in 1992 his former superior, Erich Mielke, gave a more realistic version for this move, namely, Wolf's second divorce and his private life interfered with his official duties. Wolf's constant womanizing simply did not fit in with the Puritanical attitude toward sex in the GDR. Nevertheless, Erich Honecker conferred upon Markus Wolf the Order of Karl Marx upon his retirement.[96]

During the revolution of 1989, Wolf tried to emerge as a political reformer to prevent the collapse of the GDR, but the East German masses simply did not trust him, seeing him as part of the system which they hated. On 4 November he spoke before a huge demonstration at the Alexanderplatz in East Berlin, openly admitting his past as head of the HVA and trying to protect his former colleagues. His reception was hostile, because these people associated him with the repressive domestic activity of the MfS, of which he had little or no part, even though the HVA was administratively under the MfS. The objective of the HVA was foreign espionage. He pursued his reform plan for the MfS with the new government of Hans Modrow in early December. His proposal was critical of Mielke's autocratic style and total surveillance of the population, but called for no oversight mechanisms to prevent the oppression of the past. This plan came too late for implementation, and Wolf declined his party's invitation to become a candidate for public office. He also expressed disappointment at Mikhail Gorbachev's unwillingness to intervene militarily in the GDR, as the Soviet Union had done in Czechoslovakia in 1968. Wolf felt that Gorbachev wanted to maintain his liberal image in the West at the expense of socialism in East Germany. In 1989 the GDR collapsed, and Wolf's life work, dedicated to the building of a socialist society, crumbled.[97]

In May 1990 Markus Wolf received an offer of resettlement and a large sum of money from representatives of DCI William Webster, which would have protected him from indictment and possible prison in West Germany. The

Agency needed help from Wolf to find a mole in its organization, which later turned out to be Aldrich Ames. Wolf was not ready to make himself a hostage of the CIA, however, and turned down the offer. Moreover, he would not betray anyone who had worked for him.[98] Wolf used this offer in his court appearance, where he stressed that he could have betrayed the GDR but was a man of honor.[99] In October 1990, facing an arrest warrant in the reunited Germany, he still refused an offer of immunity from prosecution from the West German government, if he would give them the names of ten to twelve of his agents and help in figuring out the damage the HVA had done to the BND. Wolf refused, since he felt a sense of responsibility to his former officers and agents.[100] When Ames was finally caught in 1994, Wolf said he was "stunned that he (Ames) could have carried on undiscovered for so long and that American counterintelligence proved so incompetent and desperate as to be forced to resort to the help of an enemy spy chief to find him."[101]

Wolf took temporary refuge in Moscow, where he found no support from his former allies in the KGB, although the head of foreign intelligence, Leonid Shebarshin, "greeted me warmly."[102] In September 1991, he surrendered to German authorities. It was unclear whether Wolf, formerly based in the GDR, could be held responsible for having conducted espionage against the Federal Republic of Germany (FRG). Although a Duesseldorf court found him guilty in December 1993 and sentenced him to six years in prison, Germany's highest court overturned the ruling on the grounds that HVA officers could be tried only for acts committed under the jurisdiction of a united Germany. A second attempt by state prosecutors in 1997 focused on a series of kidnappings rather than outright espionage and resulted in a 2-year suspended sentence. His principal memoirs, *Spionagechef im geheimen Krieg*, appeared in 1997, but an English version of this volume, though different in many respects, appeared in 1997 under the title of *The Man Without a Face*. Wolf died in his sleep on 9 November 2006 in Berlin.

WHY MARKUS WOLF SUCCEEDED SO BRILLIANTLY

Wolf was perhaps the most successful spy chief in intelligence history, certainly the most effective in the Cold War. One of his main qualities was the ability to spot the weaknesses of his enemy and ruthlessly to exploit them. For example, the dearth of men in West Germany due to the terrible losses in World War II meant that many women had to give up the idea of marriage and, in compensation, concentrate on their careers as secretaries and administrative secretaries. Wolf moved into this situation with his "Romeos," men who would seduce these women and/or marry them, thus gaining access to West German military, technical, and scientific secrets. In a more general sense he recognized universal greed and idealism, exploiting both to gain thousands of West German agents. Wolf recognized that many American servicemen and women in Germany were engaged in highly classified work, but were relatively underpaid in a large, expensive city like Berlin. He took advantage of their need, greed, and lack of morals due to a deficient American upbringing with monumental results. Wolf saw the obvious weakness of his own East Germany—the massive loss of refugees before the Berlin Wall was constructed in 1961 and laced them with his own spies sent into West Germany.

Markus Wolf had the advantage of time—34 years to learn his trade with precision and to use long-term penetration agents in West Germany, whereas in the U.S. most DCIs were removed after a few years in office or departed with a change of administration. Moreover, American intelligence officers tend to be moved around very often, before they can learn any one area in depth, whereas Wolf was able to use the expertise of long-term agents in West Germany, the area assigned to him by the Soviets. Wolf personally ran 10-12 agents, thus having a very good grasp of the problems encountered by his men and women. Consequently, he was seen as one with his officers, partially explaining why he was able to engender their loyalty and suffer very few defections.

Notes

[1] Karl-Wilhelm Fricke, *Die Staatssicherheit: DDR* (Cologne: Berend von Nottbeck, 1982), p. 187.
[2] Markus Wolf, *Spionage Chef im Geheimen Krieg: Errinerungen* (Muenchen: Verlagsgesellschft, 1997), p. 42. The purpose of the Comintern was to spread communism throughout the world.
[3] Peter-Ferdinand Koch, Die feindlichen Brueder (Muenchen: Scherz Verlag, 1994), pp. 216-17.
[4] Markus Wolf, *Man Without a Face: The Autobiography of Communism's Greaterst Spymaster* (New York: Times Books, 1997), p. 32.
[5] Koch, op. cit., pp. 224-25.
[6] Fricke, op. cit., p. 187.
[7] The Russians in Germany (Cambridge, Mass: The Belknap Press of the Harvard University Press), pp. 69-141.
[8] Wolf, *Man Without a Face*, op. cit., 40.
[9] Wolf, *Man Without a Face*, op. cit., p. 43.
[10] Koch, op. cit., p. 226.
[11] The workers' revolt was caused by impossibly high standards of production and relatively low wages.
[12] Koch, op. cit., p. 234.
[13] Wolf, *Spionage Chef* , op. cit., p. 73.
[14] The Hungarian Revolution may have been caused in part by the bitter disappointment in this icon.
[15] Wolf, *Man Without a Face*, op. cit., pp. 91-94.
[16] Ibid., p. 93.
[17] Paul Maddrell, "Western espionage and Stasi counter-espionage in East Germany, 1953-1961," *East German Foreign Intelligence*, ed. Thomas Wegener Friis, et al. (New York: Routledge, 2010), p. 26.
[18] Maddrell, op. cit., p. 25; Wolf, *Spionage Chef.*..., op. cit., p. 85.

[19] Kristie Macrakis, *Seduced by Secrets* (New York: Cambridge University Press, 2008), p. 24.
[20] These files will be discussed below.
[21] Macrakis, *Seduced by Secrets*, op. cit., p. 32.
[22] Ibid., p. 35.
[23] Wolf, *Man Without a Face*, op. cit., p. 104.
[24] Ibid., p. 101.
[25] Knabe, op. cit., p. 57.
[26] Wolf, *Man Without a Face*, op. cit., 127.
[27] Knabe, op. cit., p. 61.
[28] Wolf, *Man Without a Face*, op. cit., p. 128.
[29] Wolf, *Spionage Chef*, op. cit., p. 153.
[30] Knabe. op. cit., p.58.
[31] Macrakis, op. cit., p. 199.
[32] Ibid., p. 200.
[33] Wolf, *Man Without a Face*, op.cit., p. 143.
[34] Ibid., p. 146.
[35] Wolf, *Man Without a Face*, op. cit., p. 147.
[36] Karl-Christoph Grossmann was not related to Wolf's successor, Colonel General Werner Grossmann.
[37] Unofficial staff members are either agents or informants.
[38] Knabe, op. cit., p. 47.
[39] Jefferson Adams, *Historical Dictionary of German Intelligence* (Lanham,,MD: The Scarecrow Press, 2009), 52.
[40] Knabe, op. cit., p. 49.
[41] Ibid., p. 50.
[42] Adams, op. cit., p. 52.
[43] Knabe, op. cit., p. 49.
[44] Adams, op. cit., p. 221.
[45] Knabe, op. cit., p. 55.
[46] Ibid.,p. 67.
[47] Adams, op. cit., p. 48.
[48] Wolf, *Spionage Chef*, p. 203.
[49] Ibid., p. 218. An agent of influence is someone who "uses his or her position, influence, power, and credibility to promote the objectives of a foreign power…" Richard H. Schultz and Roy Godson, *Dezinformatsia* (Washington, DC: Pergamon, 1984), p. 38.
[50] Wolf, *Spionage Chef*, p. 244.
[51] Adams, op. cit., p. 153.
[52] Wolf, *Spionage Chef*, op. cit., pp. 286-87.
[53] Ibid., p. 186.
[54] Ibid., p. 307.
[55] Ibid., p. 308.
[56] Adams, op. cit., p. 254/
[57] Ibid., p. 462.
[58] Wolf, *Spionage Chef*, p. 313.
[59] Michael F. Scholz, "Active Measures and disinformation as part of East Germany's propaganda war," *East German Foreign Intelligence*, ed. Thomas Wegener Friis et al. (New York: Routledge, 2010), p. 117.
[60] Wolf, *Spionage Chef*, op. cit., p. 347.
[61] Norbert Podewin, *Der Rabbinersohn im Politbuero* (Berlin, 2001), p. 415.
[62] Scholz, op. cit., pp. 116-17.
[63] Guenther Bohnsack and Herbert Brehmer. *Auftrag: Irrefuehrung Wie die Stasi Politik im Westen machte* (Hamburg: Verlag GmbH), p. 31.
[64] Knabe, op. cit., p. 242.
[65] Ibid., p. 349.
[66] Ibid., p. 359.
[67] Bohnsack and Brehmer, op. cit., p. 43.
[68] Ibid., p. 37.
[69] Bernd Lippmann, "Foreign intelligence under the roof of the Ministry for State Security," *East German Foreign Intelligence*, ed. Thomas Wegener Friis et al. (New York: Routledge, 2010), p. 139.
[70] Benjamin B. Fischer, "Deaf, dumb, and blind: The CIA and East Germay," *East German Foreign Intelligence*, ed. Thomas Wegener Friis et al. (New York: Routledge, 2010), p. 48.
[71] Ibid., p. 49. Most of the CIA's Cuban agents and all of their assets in the Soviet Union since the mid-1980s were also doubled.
[72] Ibid., p. 48.
[73] Ibid., p. 50.
[74] Wolf, *The Man Without a Face*, op. cit., p.285.
[75] Fischer, op. cit., p. 53.
[76] Das Neue Berlin, Berlin, 2008.
[77] Fischer, op. cit., p. 60.
[78] Ibid.
[79] Fischer, op. cit., p. 61-2.
[80] Ibid., p. 61.
[81] Eichner and Dobbert, op. cit., p. 244.
[82] Ibid., pp. 240-i55; and Wolf, *Man Without a Face*, op. cit., p. 296.
[83] Macrakis, op. cit., p. 98.
[84] Ibid., p. 99.
[85] Kristie Macrakis, "The crown jewels and the importance of schientific-technical intelligence," *East German Foreign Intelligence*, ed. Thomas Wegener Friis (New York: Routledge, 2010), 185.
[86] The Digital Equipment Company is an American computing company.
[87] Macrakis, *Seduced by Secrets*, op. cit., p. 85.
[88] Macrakis, "The Crown Jewels and the importance of scientific-technical intelligence," op. cit., p. 188.
[89] Ibid.
[90] Ibid., p. 191.
[91] Ibid., p. 197.
[92] Ibid., p. 198.
[93] Ibid.,p. 199.
[94] Thomas Wegener Friis, "Introduction," *East German Foreign Intelligence*, ed. Thomas Wegener Friis (New York: Routledge, 2010), p. 4.
[95] Wolf, *Man Without a Face*, op. cit., p. 341.
[96] Werner Grossmann, *Bonn im Blick* (Berlin: Das Neue Berlin, 2001), p. 102.
[97] Wolf, *Man Without a Face*, op. cit., p. 3.
[98] Wolf, *Spionage Chef*, op. cit., p. 17.
[99] Wolf, *Spionage Chef*, op. cit., p. 20.
[100] Wolf, *Man Without a Face*, op. cit., p. 9.
[101] Ibid., p. 18.
[102] Ibid., p. 6.

Dr. Kenneth J. Campbell graduated from Kenyon College and received MA degrees from Johns Hopkins University and from the University of Maryland. He subsequently completed a doctorate at the University of Maryland. His area of specialization is German military intelligence. Dr. Campbell can be reached at kcamp@comcast.net.

NMIA Bookshelf

KEEPING U.S. INTELLIGENCE EFFECTIVE: THE NEED FOR A REVOLUTION IN INTELLIGENCE AFFAIRS

William J. Lahneman
Lanham, MD, Scarecrow Press. 2011.
201 pages.

Reviewed by Lt Col James E. Lightfoot, ANG, Ret, recently retired Associate Director, Center for Strategic Intelligence Research, National Defense Intelligence College. Dr. Lightfoot is the former Events Chair for the International Association for Intelligence Education (IAFIE), served 28 years with the Air Force and its reserve components, was a National Security Fellow at Harvard's John F. Kennedy School, and has written and edited numerous publications on national security and intelligence.

In the intelligence education/studies discipline, the growing body of literature has needed more publications dealing with the future of intelligence, and going beyond technological change to the broader issue of developing organizational structures and policy for a post-Cold War entity. Periodically someone rises to the challenge of attempting to pull together the disparate parts of the Intelligence Community (IC) and cover all the "INTs," be they human, signals, imagery, geospatial, or any of a growing multitude of disciplines supported by various interests. Most of these have been historical in nature. Proposing policy changes on so broad a spectrum is particularly daunting.

This is not new. Some 500 years ago Niccoló Machiavelli wrote, "It ought to be remembered that there is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things. Because the innovator has for enemies all those who have done well under the old conditions, and lukewarm defenders in those who may do well under the new. This coolness arises partly from fear of the opponents, who have the laws on their side, and partly from the incredulity of men, who do not readily believe in new things until they have had a long experience of them." This popular quotation from *The Prince* is still apt today.

William Lahneman's book is indeed such an ambitious project. As with any enormous body of knowledge, the mastery of all the material daunts anyone. Unfortunately, when advocating significant organizational change, lack of mastery invites others to pick apart the proposal. It is good that Lahneman has consulted a sizable number of experts (Jacques Gansler, William Nolte, and George Fidas, among others) readily recognizable to the Community.

In the book Lahneman proposes a "Revolution in Intelligence Affairs (RIA)." The first chapter gives a brief background on development of the IC, with emphasis on the post-Cold War era from the Clinton administration to the present. Quoting and carefully citing leading figures in national security, he notes that early on there was a lack of focus as leaders adjusted to the demise of the Soviet Union and a system built to monitor particularly one enemy, communism, and most particularly, nuclear weapons. Only with 9/11 has there been a concerted effort to change the direction, and then the requirement shifts to a much broader front; the author gives examples of nations, groups, diseases, and biopathogens. In his discussion Lahneman is careful to point out that his perspective of a need for RIA is a minority position, and that most scholars and practitioners favor an evolutionary approach.

In Chapter 2 the importance of intelligence today is covered more thoroughly, with reasons that the Community needs to make marked change spelled out. The current number one enemy is neither a military nor a state with conventional forces. The perpetrators cannot be knocked out with a nuclear weapon. To continue intelligence with a Cold War perspective is not practical.

Chapter 3 probes the development of the concept of "revolution," building on Thomas Kuhn's writings on scientific revolution and on the U.S. armed forces' approach to a Revolution in Military Affairs (RMA). With the RMA the military adjusted to the needs of DESERT STORM and changed the organization to meet new requirements and technologies. The conclusion is that the IC has not done this but needs to.

In Chapter 4 the author analyzes whether RIA is needed, or if an evolutionary method will work, and concludes that RIA indeed is needed. In Chapter 5 he goes on to explain that, if RIA is needed, so is a new paradigm, and explains why. It is, however, in the explanation of the need for revolutionary change that we run into a stumbling block. Lahneman concludes that for dealing with states the old system was pretty effective, but that it fails in dealing with terrorists and some other newer transnational issues. His proposal then seems to shift from a complete revolution to a

dual system, one that is attuned to states and the specific needs of intelligence in a more traditional sense, and a second system more attuned to open sources and ability to move with agility.

The final chapters detail how to create a new structure for U.S. intelligence. Much would remain as is, including collections and many elements of analysis. Lahneman acknowledges the difficulty of having a system that on the one hand has to keep information close-hold so that it is not leaked, yet shares information to prevent valuable parts of the puzzle from falling through the cracks, and makes specific proposals to deal with this challenge. Diagrams and graphic aids are included.

Now come the obligatory comments on shortcomings in the publication. I have two, both reflecting my own biases. The first goes back to my remark about the difficulty of dealing with the details in a wide Community. On page 117 the author states that geospatial intelligence is synonymous with imagery intelligence. This neglects geographical information systems and other techniques used. My bias stems from several years of working on new projects at the National Geospatial-Intelligence Agency (NGA). The reality is that, for many, Lahneman's remarks are correct, and particularly in the context of development during the Cold War. Still, they neglect other facets of geospatial intelligence.

The more serious concern is the already noted shift to a two-tiered approach in Chapter 5. This seems more evolutionary than revolutionary. For the first four chapters revolutionary change is strongly advocated; then in Chapter 5 Lahneman advocates both a new program and retention of the old. The two-tiered system makes sense, but is a surprise given the enthusiasm shown earlier for a revolution. My bias here comes from having a more evolutionary approach and possibly having a semantic difference with the author on where the line is between revolutionary and evolutionary.

I recommend the addition of this work to academic or personal libraries of those with an interest in policy and change in the IC. It is an easy read, something that is often a real challenge when debating policy. It also presents cogent and well-documented reasons for change, and acknowledges competing hypotheses. Bill Lahneman deserves congratulations for having the temerity to tackle such a tough issue. Though readers may not agree with all of his perspectives, they are thought-provoking and interesting. I share his concern that there is a need for aggressive reform and most of us who are veterans of working in the IC trenches know the challenges to changing such a system. This is particularly true of a system insulated from many external checks that other government agencies have to face. When it comes to change in a governmental entity, Machiavelli was right.

[Editor's Note: Dr. Lahneman is currently an Assistant Professor of Political Science at Towson University. He is also a Senior Research Scholar at the Center for International and Security Studies at Maryland (CISSM), University of Maryland School of Public Policy. He holds a PhD in international relations from Johns Hopkins University's School of Advanced International Studies (SAIS), an MA in national security affairs from the Naval Postgraduate School, and a BS from the U.S. Naval Academy.]

• •

THE TECHNICAL COLLECTION OF INTELLIGENCE

Robert M. Clark. Washington, DC, CQ Press. 2010. 313 pages.

LTC Christopher E. Bailey (USAR, Ret) is a faculty member at the National Defense Intelligence College specializing in national security law, processes, ethics, and strategy. Licensed to practice law in California and the District of Columbia, he is a member of the National Security Law Division, American Bar Association.

Dr. Robert M. Clark, a retired intelligence officer with 36 years of experience, has prepared an outstanding introductory work on the technical collection of intelligence that demystifies the field. Clark has a long career in technical intelligence. With a doctorate in electrical engineering (as well as a law degree), he served at the Central Intelligence Agency (CIA) as an analyst and Chief of the Directorate of Intelligence's Analytic Support Group, where he worked on a range of issues such as Soviet radar, communications, and electronic warfare systems. Later, he was the President of the Scientific and Technical Analysis Corporation (STAC), where he organized and directed intelligence collection and analysis support efforts, and developed new collection and analysis methodologies. Dr. Clark is also the author of *Intelligence Analysis: Estimation and Prediction* (1996) and *Intelligence Analysis: A Target-Centric Approach* (first published 2003, updated since), among other works.

Dr. Clark has provided a well-organized and clearly understandable introduction to what is often an arcane topic to non-technical persons. He defines technical collection as the collection, processing, and exploitation of "non-literal information," which he defines as information in a form not used for human communication. In other

words, non-literal information requires special processing beyond the translation and analysis of collected information that an analyst ordinarily encounters in the form of human intelligence, open source, and most communications intercepts. In practice, this means that the book is focused on measurement and signatures intelligence (MASINT); certain forms of signals intelligence (SIGINT), such as foreign instrumentation systems intelligence (FISINT), and electronic intelligence (ELINT); imagery intelligence (IMINT); and missile and space intelligence.

The author has organized the book into twelve separate chapters, with some chapters devoted to special topics and others to specific intelligence disciplines. For example, some chapters focus on topics such as "Collection Platforms" or "Managing Technical Collection," while others examine "Optical Imaging" or "Missile and Space Intelligence." Each chapter is filled with facts, informative examples related to problems faced by intelligence collectors and analysts, and detailed discussions in language understandable to a person with a non-scientific background. In addition, a very useful table of acronyms can be found at the front of the book, while at the back there is an equally useful glossary of terms. In short, this is the perfect textbook for scholars and budding intelligence officers who need to understand the technical terminology, collection systems, and capabilities, and the work involved in processing and producing technical intelligence.

This book has particular utility for intelligence officers, such as political-military analysts, who work with technical products on an occasional basis. Dr. Clark shows how an enterprising intelligence analyst can use technical systems, processes, and products to provide relevant all-source products to consumers. On one hand, various technical systems can overcome adversarial denial and deception, establishing a closer approximation to "ground truth." Thus, the all-source analyst can have a sense for the reliability and importance of the evidence with which he is working. On the other hand, the all-source analyst can provide relevant tip-offs for technical collectors, permitting the economical use of scarce resources. Here, the all-source analyst might direct the collection manager's interest to a particular time or place, or might opt for commercial imagery in place of scarcer high-resolution products. Also, Clark provides numerous historical examples, such as the Bruvenal Raid during World War II, in which collaboration facilitated unique and refined work.

Dr. Clark provides an informative introduction to many unique collection systems, explaining both system capabilities and limitations. For example, he details how various satellite systems, both government and commercial, operate to provide optical, spectral, and radar coverage. He explains how various acoustic systems operate to track submarine, surface ship, nuclear, and earthquake activity. He also outlines how specialized collection systems, such as Cobra Dane or clandestine SIGINT, work to provide focused collection. Here, he offers relevant case studies, such as showing how specialized equipment was utilized to locate a Soviet submarine that sank in March 1968, facilitating its later recovery by the *Glomar Explorer*. Moreover, he provides the reader with an important introduction to biometrics, an emerging field that has demonstrated great utility in Iraq and Afghanistan. The book is filled with useful definitions, diagrams, charts, and photographs in side-by-side comparison with imaging products, making the entire topic clearly understandable to the non-technical intelligence officer.

All said, this book is a fine introduction to intelligence collection systems, processes, and products, as well as a useful desk reference for people who work with technical collection on an occasional basis.

• •

NATIONAL SECURITY IN THE OBAMA ADMINISTRATION: REASSESSING THE BUSH DOCTRINE

Stanley Renshon. New York, NY, Routledge. 2010. 291 pages.

Reviewed by Daniel W. Opstal, an analyst at the National Geospatial-Intelligence Agency and a July 2011 graduate of the National Defense Intelligence College, earning a Master of Science of Strategic Intelligence (MSSI) degree. He also serves as an adjunct professor at American Military University.

The political opening surrounding the Arab Spring, the recent NATO-supported raids on Libya, and Osama bin Laden's demise in Pakistan make Dr. Stanley Renshon's reassessment of the Bush Doctrine in the context of the Obama administration a very timely look at the psychology of an administration's strategic worldview. The Bush Doctrine is defined in this work as a set of strategic premises, outlined primarily in the National Security Strategies (NSS) of 2002 and 2006. The Bush Doctrine has three key themes: American primacy, assertive realism, and stand-apart alliances. Dr. Renshon explores the formation of the Bush Doctrine, its contributions, limitations, and continued implementation by the Obama administration. This lends itself to comparison with the current administration's recent actions on the world stage.

American primacy is a strategic worldview that holds that America is and should remain a preeminent world power, with global responsibilities. Renshon notes that this is interpreted as empire-building when it has a broader meaning of ensuring economic and political stability. President Obama is characterized as agreeing that the U.S. needs to continue to be in a leadership role on the world stage but that, to paraphrase John F. Kennedy, not every problem can have "an American solution" (p .43). This Wilsonian aspect of the Bush Doctrine is seemingly carried over in the Obama administration with regard to Libya. The President used authority derived from United Nations Security Council Resolution 1973 to order U.S. forces to protect Libyan civilians using both aerial bombardment and a no-fly zone. Yet, Renshon states the UN is an unreliable and unaccountable ally, and as of this writing President Obama's actions are being investigated by Congress as a possible violation of the War Powers Act (p. 50).

This offensive stance on national security carries over into the second theme, assertive realism. Assertive realism is the belief that the United States should have an offensive, even preemptive, stance on national security. Given the contentious nature of the Afghanistan and Iraq conflicts under the Bush administration, this seems an understatement. The doctrine of preemption is analyzed by Dr. Renshon, who rebuffs what he perceives as the myth of the Bush "cabal" that ran the White House's foreign policy. In other words, he believes that President Bush, although inexperienced in foreign affairs at the beginning of his presidency, did not simply roll over on policy decisions and learned quickly. This is reflected by his addressing the U.S. and coalition's role in ensuring Iraq post-conflict stabilization activity in his 2006 NSS (it was not mentioned at all in the 2002 NSS). Renshon's description of President Obama as an inexperienced but highly decisive leader in his policy discussions comes across as a veiled critique, leading the author to warn his reader about the dangers of overconfidence (p. 69). President Obama's decisiveness, however, seems to have paid off with the successful raid on the Osama bin Laden compound in May 2011. Yet, this was made possible, in part, through the steadfast leadership of a Bush-era appointee in the post of Secretary of Defense and a closer union between DoD and CIA.

A final theme of the Bush Doctrine is stand-apart alliances. A stand-apart alliance is an umbrella term for the politically charged phrase "coalition of the willing," which is inexorably tied to the Bush Doctrine. Both Presidents Bush and Obama built coalitions of various types that are not tied to the formal United Nations structure. Renshon spends a significant amount of time defending the lesser-known Bush coalitions that were highly successful, such as the partnership with Belgium and other nations on countering terrorist finances and the Proliferation Security Initiative with Russia. This is certainly an area where there was a definite change in the administration. This is perhaps the fourth and final theme in his book – an overview of the various options for what should replace the Bush Doctrine.

Francis Fukuyama, a noted scholar of international relations, is quoted by Renshon as calling for "Realistic Wilsonianism" to replace the Bush Doctrine in deference to the liberal worldview of a world fundamentally connected on multiple economic and political fronts. Renshon, who provides a variety of assessment methodologies of international policies in the book, looks for glimmers to see what the Obama doctrine will encapsulate. He notes that President Obama is a man of vast "domestic ambitions" and inherits a Congress bitterly divided by partisan strife on both foreign and domestic issues (p. 211). This, too, will shape his decision making. If Renshon were writing this book today, perhaps he might mention the massive impact of the national debt.

Overall, Dr. Renshon asks that President Obama consider the Bush Doctrine's premises and themes, while imperfect, as part of his strategy calculations. Thus far, it appears this has occurred, despite marked differences on what constitutes a stand-apart alliance or coalition (e.g., Iraq versus Libya). Dr. Renshon's psychoanalysis of the Bush Doctrine is a useful set of guidelines to understand the state of U.S. foreign policy during President Obama's first few months in office. In reflecting on recent events, his words are fairly prescient as the emerging Obama doctrine continues to take form.

• •

THE NATIONAL SECURITY ENTERPRISE: NAVIGATING THE LABYRINTH

Roger Z. George and Harvey Rishikof, eds.
Washington, DC, Georgetown University Press. 2011.
350 pages.

LTC Christopher E. Bailey (USAR, Ret) is a faculty member at the National Defense Intelligence College specializing in national security law, processes, ethics, and strategy. Licensed to practice law in California and the District of Columbia, he is a member of the National Security Law Division, American Bar Association.

Roger George and Harvey Rishikof have brought together a series of outstanding articles from leading authorities in the national security policy and intelligence communities. *The National Security*

Enterprise is a ground-breaking textbook that provides students with a comprehensive view of the national security community, to include seldom-examined areas such as the role of the Office of Management and Budget (OMB), the federal judiciary, lobbyists, think tanks, and the media. Moreover, this book is unique and valuable in that it examines each member, partner, rival, or player from its individual cultural perspective. For example, what is the cultural perspective of OMB and what does that office bring to the table? Or how does OMB's view of its role and perquisites compare to that of the Federal Bureau of Investigation (FBI) and what it brings to the table? In short, this work is an ideal introductory textbook for new students in security studies trying to understand the overall national security architecture before diving into niche areas of interest.

Dr. George is a professor of security studies at the National War College and an adjunct professor at Georgetown University, where he teaches in the Security Studies Program. He was a career intelligence analyst at the Central Intelligence Agency (CIA) for more than 30 years and was a member of the Senior Analytic Service (SAS). After a long legal career, Mr. Rishikof has been a professor of law and national security studies at the National War College since 2004. He specializes in national security law, civil and military courts, terrorism, international law, civil liberties, civil-military relations, governmental process, and the U.S. Constitution. Both have published extensively on intelligence and national security.

The National Security Enterprise takes a comprehensive, in-depth approach to understanding the national security community as a whole, including institutions, people, processes, laws, and issues. The contributing authors include Thomas Fingar, who served as the first Deputy Director of National Intelligence for Analysis; Jonathan Hoffman, who served as a deputy assistant secretary in the Department of Homeland Security (DHS); the former director general of the Foreign Service and Ambassador to Turkey; and other distinguished academics/former senior officials.

This book is organized into three major sections: The first section is "The Interagency Process," with chapters on the process itself, the National Security Council, OMB, the State Department, the Office of the Secretary of Defense (OSD), the military, ODNI, CIA, FBI, and DHS. The second section is "The President's Partners and Rivals," with chapters on the U.S. Congress and the Supreme Court. The third section is "The Outside Players," with chapters on lobbyists, think tanks, and the media. The book concludes with a chapter by Rishikof and George that is both a summary and analysis and aptly titled "Navigating the Labyrinth of the National Security Enterprise." The book also provides readers with heavily end-noted chapters loaded with important facts, organizational charts, anecdotes, and analysis of key issues. For example, Frederick Smith and Franklin Miller have authored an informative chapter on OSD with an overview of the organization over time, the impact of the Goldwater-Nichols legislation, the differing perspectives on political appointees versus careerists, and the role of generational change. In a second example, Gary Schiffman and Jonathan Hoffman have a useful chapter on DHS, showing how the varied institutions of homeland security have been evolving.

The National Security Enterprise is also unique in terms of thinking about intelligence oversight, a problem typically conceived in terms of either executive (i.e., programmatic), Congressional (i.e., accountability and spending), or judicial (i.e., legality) realms. In addition to the standard issues, this book provides a comprehensive view of oversight including, as noted, often overlooked but key actors, often with a fresh perspective, such as OMB, think tanks, and the media. For example, the media, while often criticized for publishing information considered inimical to national security, are analyzed by looking at the "tribes of national security media" and at situations where there is pronounced media influence on policy events.

This is a "must have" book for budding national security professionals.

A WOMAN'S WAR: THE PROFESSIONAL AND PERSONAL JOURNEY OF THE NAVY'S FIRST AFRICAN AMERICAN FEMALE INTELLIGENCE OFFICER

Gail Harris, with Pam McLaughlin.
Lanham, MD, Scarecrow Press. 2010.
270 pages.

Reviewed by Marilyn B. Peterson, a master instructor at the Joint Military Intelligence Training Center (JMITC), DIA; adjunct professor at University of Maryland University College (UMUC), a leading provider of on-line intelligence education; and former Chair of the International Association for Intelligence Education (IAFIE). The views expressed below are solely those of the reviewer and do not reflect the official positions of the U.S. government, DoD, DIA, or JMITC.

In the 1970s, women were a rarity in combat positions of the U.S. armed forces. Nonetheless, Gail Harris was assigned by the U.S. Navy to a combat intelligence job in 1973; she was the first African-American female to hold such a position. From there, she rose to be a Navy captain, the highest-ranking African-American woman in the Navy in 2001.

This autobiography is part personal journal, part motivational speech, part history, and part how women began to play key roles in the intelligence field. Several chapters utilize footnotes and sources, resulting in the material reflecting an almost conversational mix of facts and perceptions. The end of each chapter also includes a list of key points and "takeaways." Some might call it a "chick book," written with humor, honesty, and a sense of history, but decidedly by a woman.

This chronologically-ordered book takes us from Dr. Harris' childhood, growing up in Newark, NJ, to her retirement in 2001. She was strongly influenced by the movie, *Wing and a Prayer*, at age five, and decided she wanted to be a Naval intelligence officer. Her parents moved to suburban New Jersey by the time she went to high school, and she went on to Drew University in Madison, NJ. While there, she became interested in international studies and received a scholarship for a 2-year graduate program in international studies in Denver, CO. It was this interest that led her to become a test case for female intelligence officers in operational squadrons.

During her first few years in the Navy, Harris attended Naval Intelligence Training School and prepared to be one of the first female intelligence officers in an operational squadron. Being a good student who did her research, the analysis itself was not the hardest part; it was "fitting in." Gradually, the men in service grew accustomed to having a female in their workspace and overcame their discomfort and, sometimes, resentment.

As someone who was often the lone female in a large group of law enforcement officers at work or in conferences, this reviewer can certainly relate to this situation. I doubt that I would be as frank in print as the author is about some of the shenanigans that occurred, but they were similar.

While in the Navy, Harris served in Alaska, Hawaii, Japan, Kosovo, Spain, Egypt, and Ireland. In each place, she learned not only about the country and the military situation, but more about how she could adjust and relate to new surroundings.

The author stresses the importance of mentors in her life. Not surprisingly, all of them were men, starting with her father. Among the mentors who influenced her was Admiral William Studeman, who served at the Naval War College with her (he was then a captain). [Editor's Note: ADM Studeman is a former Director of NSA, former Deputy DCI, and current member of the National Defense Intelligence College Board of Visitors.] Another individual with whom the author shared ideas along the way was a young Condoleezza Rice, who was studying toward her doctorate in international relations at the University of Denver.

During her career, CAPT Harris was an intelligence officer, a watch officer, a member of the Iraqi Crisis Action Cell, and a leader in the cyber warfare area. Throughout these different positions at different times, she experienced incidents where her efforts led her perilously close to court-martial yet certainly resulted in promotion and respect. This dichotomy is also not unusual in this field.

The book is full of ideas, advice, historical moments, and life. It is not a heavy read, and can be picked up and put down over a period of time without losing its value. In some ways, it provides a reality check to those thinking of joining the armed forces; for others, it is a story of determination, perseverance, spirituality, and success.

NOTE: This book is part of the Scarecrow Professional Intelligence Education Series (SPIES), edited by Dr. Jan Goldman, a former longtime faculty member at NDIC who now teaches at the FBI Academy. It was written by CAPT (Ret) Gail Harris "with" Pam McLaughlin, a ghost writer.

HISTORICAL DICTIONARY OF NAVAL INTELLIGENCE

Nigel West. Lanham, MD, Scarecrow Press. 2010. 406 pages.

Reviewed by CDR (USNR, Ret) Cal Carnes, a 35-year IC veteran with DIA, FBI, Naval Investigative Service, the IC Staff, and Army counterintelligence as a CI officer; also a CI contractor with DIA's Defense HUMINT Service and DoD's Counterintelligence Field Activity. Holding master's degrees from Georgetown University in National Security Studies and the National Defense Intelligence College in Strategic Intelligence, he is a longtime member of the NMIA Board of Directors.

Naval intelligence services have been foremost in a number of major countries throughout history. Before the formation of the British Secret Intelligence Service (MI6), the Naval Intelligence Division created in 1887 gathered most of the foreign intelligence for the United Kingdom. Even when MI6 was formed in 1909, its first head was a Navy Captain, Mansfield Cumming, apparently due to the fact that the British valued the services of a naval officer in intelligence. The U.S. Office of Naval Intelligence was officially formed in 1882, the first organized intelligence service for the United States and the longest serving intelligence organization. This was before the formation of Army Intelligence in 1885, and the first centralized intelligence organization, the Office of Strategic Services, in World War II. Until recent times, the Soviet Union/Russia had a separate naval intelligence component, independent of the GRU and the KGB, revealed through the Venona intercepts, with its own special forces, Naval SPETSNAZ. The Soviet Navy even had a separate residency for spying here in the United States during World War II, in addition to the residencies of the KGB and GRU.

Therefore, the significance and role of naval intelligence is apparent. This historical dictionary is hence of immense value; its importance cannot be overstated. The dictionary is most comprehensive and covers many topics with which I was unaware, on U.S., British, and German naval intelligence. For example, I knew nothing about the American secret wartime intelligence unit, Atlantic Section, Combat Intelligence Division, U.S. Fleet, in World War II, or of Otto Kuehn, the German naval officer who spied for the Japanese in Hawaii.

I am particularly pleased to see various foreign espionage topics covered. The topic of Auxiliary, General Intelligence (AGI) ships as unique Soviet naval platforms for intelligence collection is interesting and important (I had that "account" while with the Soviet Navy Section, DIA). Commander Dieter Gerhardt, South African Navy, not well known, spied for the GRU for 23 years (a book will soon be out on the subject). The exposure of Commander Eugene Ivanov, GRU and naval attaché to London, led to the Profumo scandal of 1964. The Soviet Naval GRU, usually an unknown service, was an independent organization with its OSNAZ, signals intelligence arm. Stephen Joseph Ratkai worked for both Hungarian intelligence and the GRU as Captain Boris Tatarintsev, assistant naval attaché to the Soviet embassy in Ottawa, ran Ratkai. The espionage case of Glenn Souther, at Fleet Intelligence Center, Europe and Atlantic (FICEURLANT), Norfolk, Virginia, supposedly spying for Russia and defecting there, is unique and unsolved (I have visited FICEURLANT for conferences). The episode of Jay Pollard spying for Israel is significant (he and I worked for the Naval Investigative Service (NIS) when I was there from 1984 to 1986, but apparently for different masters). A Chinese espionage case covered in recent counterintelligence conferences, the Chi Mak case, is important and indicates a significant threat to U.S. Navy technical information. The entry for Nikolai Artamonov, aka Nick Shadrin, does not include his initial employment with the Naval Scientific and Technical Intelligence Center (NAVSTIC) at the Naval Observatory, a period when he felt he made more of a difference. I knew Nick as a defector at DIA and invited him to one of my Naval Reserve intelligence meetings. I was surprised to see information on the Special Navy Control Program (SNCP) released. When I served in the DIA Soviet Navy Section, we jokingly called it "Sneak-Up."

I found some discrepancies while examining the dictionary. While mentioned briefly in the text, NIS—now the Naval Criminal Investigative Service (NCIS)—in my opinion should have had a separate notation. Somewhat independent with its criminal investigative responsibilities, NCIS nevertheless is a key component of the U.S. naval intelligence family with major counterintelligence functions. When I left NIS to transfer to the Army, I received a shadow box with the NIS logo which clearly had "Naval Intelligence" on it.

The dictionary being somewhat British-centric, I find it noteworthy there is no mention of the London NIS field office (used to be the regional office) in Eastcote, on the northwest outskirts of London, originally a GCHQ base in World War II, or the old NIS field office in Kensington, downtown London (no longer active). I served in both offices on reserve duty in 1990 as an NIS Officer/Agent. The regional NIS office moved to Naples, Italy. I first met Nigel West during that period when he was a Member of Parliament at the House of Commons. Subsequently, I met the author on a number of other occasions, including the Spy Tour of Moscow in 2003, and consider him a friend.

I also find it somewhat unusual there is no notation for the massive Commander-in-Chief, Naval Forces, Europe (CINCUSNAVEUR) building across from the U.S. Embassy in London on South Audley Street. It is now U.S. Naval Forces, Europe (USNAVEUR), and moved to Naples, Italy. The N-2 there had a significant intelligence capability (made temporary duty, or TDY, visits to the site). There is also no notation for the U.S. Joint Analysis Center (JAC), RAF Molesworth, UK, where I also was on TDY.

Neither the Navy and Marine Corps Training Center (NMITC) in Virginia Beach, Virginia, nor the Fleet Intelligence Training Center, Pacific (FITCPAC), in San Diego, California, is in the dictionary. NMITC in particular has a very major role to play in U.S. naval intelligence and includes the Center for Naval Intelligence. I made a visit to NMITC last summer, and was given a special tour of the facility and the surrounding area by the Marine Corps executive officer of the school.

I had some problem with the acronyms included in the section on the Fleet Intelligence Center. The U.S. Navy is in love with acronyms. Rather than JCPA, it was the Joint Intelligence Center Pacific Ocean Area (JICPOA) formed in 1943. Fleet Intelligence Center Pacific (FICPAC) was the correct acronym, rather than FINPAC; then it became JICPAC (Joint Intelligence Center, Pacific). I received a JICPAC award coin after briefing there on TDY in the early 1990s. Fleet Intelligence Center, Atlantic (FICLANT) is the proper title, rather than FICATLANT. The correct acronym is FICEURLANT, noted earlier, rather than FICEURATLANT. FICEURLANT became Atlantic Intelligence Command (AIC), where I did my last reserve intelligence training duty in August 1991. The AIC then became a Joint Intelligence Center under Joint Forces Command. The JICs have since been expanded and redesignated Joint Intelligence Operations Centers (JIOCs).

In describing Task Force 157, a Navy HUMINT organization, headquartered in Rosslyn, Virginia, the building where the headquarters was located is "Pomponio," rather than "Pampanio." There were TF 157 offices elsewhere. DIA at one time had its Defense Attaché oversight offices in the building when I visited there. Related to the TF 157 organization, I once supported Task Force 168 as a reserve HUMINT operations officer.

It makes sense to have a list of U.S. Navy signals intercept sites. However, the site at Augsburg, aka Gablingen, and Bad Aibling, Germany, were Army Intelligence and Security Command (INSCOM) sites, although some Naval Security Group (signals) liaison personnel possibly were stationed there. I was at Gablingen for a week in the early 1990s, working for Army intelligence. Some other sites could have been identified to add to the study, such as the location of various naval intelligence headquarters and associated facilities in the UK, the U.S., and other countries.

An excellent bibliography on naval intelligence is offered, although I would add the following to the list: *The Office of Naval Intelligence: The Birth of the First Intelligence Agency, 1865-1918*, and *Conflict of Duty: The U.S. Navy's Intelligence Dilemma, 1918-1945*, by Jeffery M. Dorwart; *Double-Edged Secrets: U.S. Naval Intelligence Operations in the Pacific during World War II*, by W.J. Holmes; *Special Agent, Vietnam: A Naval Intelligence Memoir*,by Douglass H. Hubbard, Jr.; *Lonely Vigil: Coastwatchers of the Solomons*, by Walter Lord; and *The Silent War: A History of Western Naval Intelligence*, by Richard Deacon.

Reviewing a dictionary is difficult. One must go over each entry and examine it based on one's knowledge and experience, hoping not to miss something. The changes I have identified here have to be considered of relatively minor importance.

This is the first dictionary devoted solely to naval intelligence. Examining the dozen or so intelligence dictionaries and encyclopedias in my personal library, various naval intelligence topics are covered, but not one of them addresses the subject of naval intelligence as a major theme. The historical dictionary covers subjects not covered anywhere else and is not redundant with any other reference sources.

The historical dictionary is a most interesting read of a very important and timely subject. It identifies numerous items on naval intelligence, many heretofore unknown to this reviewer. The dictionary is a very useful reference allowing for the study of naval intelligence. It would be a welcome addition to the libraries of any with an interest in this topic, but particularly for naval intelligence professionals in the UK and the U.S.

• •

CHALLENGES IN INTELLIGENCE ANALYSIS: LESSONS FROM 1300 BCE TO THE PRESENT

Timothy Walton. Cambridge, UK, and New York, NY, Cambridge University Press. 2010.
308 pages.

Reviewed by Lt Col (USAF) Richard Cimino, National Defense Intelligence College Senior Service Advisor and faculty member focusing on globalization, economics,

and joint professional military education, who good-naturedly refers to his review as "a romp through history from an analyst's point of view."

It was September 1974, and a metallurgist from Pakistan decided he would help his country do the impossible: develop its own nuclear weapon development capability. He was educated in Belgium, and then hired by a Dutch company involved in uranium enrichment. By December 1975, A.Q. Khan had jumped ship, arriving back in Pakistan with centrifuge blueprints and contact information for dozens of centrifuge supply companies. That this individual could propel a nation into the nuclear club is significant. That this individual could also *independently* assist Iran, Libya, and North Korea in developing nuclear weapons is dramatically more significant. U.S. Intelligence Community analysts and their allies overlooked A.Q. Khan as he built Pakistan's "Islamic" bomb. However, the analysts did score a success when they uncovered his proliferation activities and even prompted the government of Pakistan to place Khan under house arrest in 2004. The conventional wisdom among analysts in the 1970s and 1980s was that only governments could successfully develop and proliferate nuclear weapons technology. Realizing that a super-empowered individual could also develop and spread nuclear weapons know-how, creative analysis in the late 1990s and early 2000's enabled the breakthroughs that led to discovering and shutting down Khan's network. Was it a little late? Maybe. Was the analytical success too late to matter? Absolutely not. Shutting down A.Q. Khan's network stopped many countries in their tracks and even reversed Libya's WMD direction.

What was it about the strategy to discover and bring down the A.Q. Khan network that worked, and can these elements be replicated to succeed in similar problems? This is what analysts today need to ponder and think about. Timothy Walton's book *Challenges in Intelligence Analysis* provides 39 case studies which explore historical events from the analyst's perspective. There is no better primer on major situations throughout history that were made or broken based on the ANALYSIS involved. Cases include the use of spies by Moses, Stalin's assessment of Hitler prior to Germany's invasion of Russia in WWII, the breaking of the American Mafia in the 1980s, and Japanese car companies' analysis of the U.S. auto market. Whether you are an intelligence professional, a business or financial analyst, or simply interested in history, this book will grab and hold your attention case after case. Many nights I found myself saying, just one more chapter…oh, I'll just read this next story about the Colombian drug cartels…etc.

Timothy Walton potentially has a hit on his hands, although his academically designed *Challenges in Intelligence Analysis* will probably never be a bestseller because it is written as a college textbook. It is similar to Robert Greene's *48 Laws of Power* (Viking, 1998), where each law is described and then illustrated with historical examples. Walton's book ends each case study with questions for further thought and recommend readings. These are great tools for academic instructors, but not so great for the common reader. Walton could revise this book to attract the common reader. Cambridge (the current publisher) or a different publisher stands to generate great sales if it can help Dr. Walton adjust his book to appeal to a mass audience. It would resonate with the Malcolm Gladwell/Simon Winchester crowd.

The lessons are short stories of historically significant events. The stories emphasize the information at hand for the decision-makers, and allow students/readers to evaluate the decision- maker's background or the situational context for relevance. Sometimes the intelligence support apparatus is covered, allowing insight into how effective governments/corporations might organize their own intelligence support structures, and at other times a government's failure to do so is covered, with dire consequences.

Challenges in Intelligence Analysis can serve as an endless jumping-off point for most any professor of the humanities. For example, nearly any historian can find a case that falls into his time period of interest and, with Walton's recommended readings and questions for further thought, an entire course could be developed. Professors will delight in such cases as Walton's descriptions of how Caesar used intelligence analysis to conquer Gaul, how George Washington was his own intelligence officer (to great success), and how the Intelligence Community largely missed the collapse of the USSR.

These lessons are fantastic snippets of history that can grab and hold the attention of a recreational reader. Whereas these cases may seem short and slightly superficial to some, the recreational reader may find them engaging and insightful—it all depends on one's perspective. One can picture a retired gentleman reading this book with intellectual curiosity and find enjoyment in his exploration into the employment of analysis in a given situation. Graduate and undergraduate students alike would welcome this book as required reading, as it serves up information about some of the most significant events in human history—quickly, eloquently, and to the point. Analysis matters (history tells us so), and this book shows us how.

Some may criticize Walton for trying to cover cognitive biases and historical cases, doing neither very well. However, I feel the author has struck exactly the right balance. If one wants a more in-depth study of cognitive

biases, then read Richards Heuer. If one wants more historical details about some of the cases Walton uses, then read the history books. Walton lists many references at the end of each chapter. This is an easy book for learning the initial details and then completing further study, if one so desires.

This book is praised by Loch Johnson and Christopher Andrew, highly respected editors/authors in the field of intelligence studies literature. It is a must read for intelligence professionals. It is another outstanding example of the body of work from those associated with Mercyhurst College, one of the oldest and most established of the civilian intelligence studies programs. Heads-up for my students: I am ordering several copies for classroom use. I hope my students will go on to uncover nefarious actors like A.Q. Khan sooner rather than later.

[Editor's Note: Dr. Walton holds a BA degree from the College of William and Mary and a PhD from the University of Virginia. After serving in the Navy, he was an analyst at the CIA for 24 years. Since retiring, he has taught analysis at the Sherman Kent School, Mercyhurst College's program in the Washington, DC, area, and the Director of National Intelligence Office's *Analysis 101* course. He will be joining the faculty at James Madison University this fall.]

Review Essay:

A Comparative Look at Intelligence Writing and Usage Guides

Reviewed by Kel McClanahan, Executive Director of National Security Counselors and Associate Editor, *AIJ*.

Titles reviewed in depth:

Communicating with Intelligence: Writing and Briefing in the Intelligence and National Security Communities. James S. Major. Lanham, MD, Scarecrow Press, 2008. 420 pages.

Writing Classified and Unclassified Papers for National Security. James S. Major. Lanham, MD, Scarecrow Press, 2009. 234 pages.

Titles reviewed in brief:

Style: Usage, Composition, and Form (2nd edition). James S. Major. Washington, DC, Defense Intelligence Agency, 2004. 255 pages.

Citation: Note and Bibliographic Form (2nd edition). James S. Major. Washington, DC, Defense Intelligence Agency, 2003. 198 pages.

Style Manual and Writers Guide for Intelligence Publications (6th edition). CIA Staff. Washington, DC, 1999. 248 pages.[1]

Analyst's Style Manual. Bill Welch, ed. Erie, PA, Mercyhurst College Institute for Intelligence Studies Press, 2008. 40 pages.

SIGINT Reporter's Style and Usage Manual. National Security Agency, 2010, available at http://www.governmentattic.org/4docs/NSA-SIGINT-style-manual_2010.pdf.

A year or so ago, I obtained review copies of two books by James Major, titled *Communicating with Intelligence* and *Writing Classified and Unclassified Papers for National Security*. Prior to receiving these books, I personally had been relying on more general style manuals, such as the *Chicago Manual of Style* and the legal manual known as the *Bluebook*, and supplementing anything written about intelligence matters with the CIA's *Style Manual and Writers Guide for Intelligence Publications*. Upon reading Major's two books, I decided that it would be of interest to *AIJ* readers if someone were to do a comparative review of all of the intelligence and security-related style manuals out there, allowing for the construction of a comprehensive set of style rules for intelligence professionals. Now, a year later, as I write this review, I can safely say that I have never found a discipline with as many competing styles and

standards as intelligence, and my original goal is for now beyond my grasp. However, what I can do here is provide a roadmap of the strengths and weaknesses of each of the texts I reviewed, allowing our readers to intelligently choose the best book for the job before them on a case-by-case basis.

In general, these texts can be divided into two main categories, which I term "Writing Guides" and "Usage Guides." "Writing Guides" discuss the *manner* of writing for intelligence audiences, with general lessons for general purposes, while "Usage Guides" are more like dictionaries of how to spell certain problematic words and how to use certain categories of terms. While a few of these books do encompass both categories, they almost always do so in separate parts of the book, which allows us to easily discuss the "Writing Guide" portions separately from the "Usage Guide" portions.

I. WRITING GUIDES

A. *Communicating with Intelligence*

If I could assign people in search of a national security writing guide one book to read, it would be this one. It is very fitting that this book was Volume 1 in the Scarecrow Professional Intelligence Education Series ("SPIES") put out by Scarecrow Press (*AIJ*'s Summer 2010 issue included a review of Volume 6: David Perry's *Partly Cloudy: Ethics in War, Espionage, Covert Action, and Interrogation*, and two others are slated for review in future *AIJ*s), as it establishes a clear set of ground rules that any intelligence educator or student should follow. Moreover, it is not a coincidence that four of the texts I reviewed were written at different points in time by James Major; he has been involved in the training of intelligence writers for longer than most intelligence writers have been writing. If I could in fact choose one *source* of any kind for a burgeoning intelligence writer, I would recommend hiring Major to stand over his shoulder and teach him everything he knows. [Editor's Note: After retiring from the Army many years ago, Mr. Jim Major created the Writing Center at the then-Joint Military Intelligence College (JMIC). He retired from government service at the end of 2005, and the Writing Center that was his "baby," what was left of it anyway, has since been folded into the current NDIC Center for Strategic Intelligence Research.]

This book excels at its mission for three reasons. The first is that it is written in a Goldilocks-style fashion that is not too pedantic for students or other writers new to the field, while remaining not too patronizing for seasoned professionals. Major writes in an admittedly casual style that evokes the image of a lecturer pacing back and forth in front of a projector at an orientation seminar, but he accomplishes his goal. His examples are realistic and immediately relatable, primarily because he shamelessly and openly steals them from papers that have been handed in by his students over the years. And his exercises are interesting and thought-provoking enough to make the reader actually give some thought to them, rather than just skimming them over and reading the answers. Overall, reading this book is more like listening to a lecture at a conference than reading a textbook, which to me is a good thing, especially when it addresses an inherently eye-glazing topic like writing style.

The second reason for this book's success is the way in which Major teaches the same information several times in myriad fashions, such as descriptions, charts, visual aids (the "balloon maps" and "idea trees" in Chapter 4 and the "paragraph-as-mobile" graphic in Chapter 5 are particular favorites), and exercises. As any educator knows, the more ways you can present the same information to a student, the more likely he is to understand it. Major understands this to a "T," and the particular genius of this book is that the book *itself* is an example of all of the techniques he is seeking to teach the reader. For instance, Major teaches the effective use of visual aids in intelligence products, while simultaneously "practicing what he preaches" throughout the book. This type of "meta-teaching" allows the reader to learn by example by the very act of reading the book, providing yet anther delivery system for the lessons.

The third and final reason for this book's success is that nothing in it is really *new*; it is just packaged into a new pedagogical style. Some of the book's most insightful lessons seem obvious once you read them, but they represent the idea that if something goes without saying, *nobody says it*, and as a corollary, *nobody even thinks about it.* Certain such pearls of obvious wisdom that are nonetheless frequently ignored by writers include

- "[A]void the techniques that cause you to lose interest in [someone else's] writing or simply to consider it bad writing." (p. 145)
- "Every style has its time and place, and the trick is adapting your own techniques to suit the task at hand and the intended reader of your product." (p. 152)
- The seven different orders of logic that can be used (pp. 154-157)

Major has found an effective way to teach a very boring topic in such a way that even people who think they already know everything about it will still continue reading. Given how many intelligence professionals are subject matter experts who write for a living, such a presentation is key.

Before moving on to the next book, it is worth noting that *Communicating with Intelligence* also includes an excellent

discussion of one particular type of writing that is not mentioned in the others – how to review someone else's work. Chapters 6 and 7 both bear close reading on this subject.

B. *Writing Classified and Unclassified Papers for National Security*

This book was written as a complementary SPIES volume to *Communicating with Intelligence*, and as such it accomplishes its goal. Where *Communicating with Intelligence* takes more of a bird's-eye view of intelligence writing style, this book is buried in the weeds, but in a way that does not detract from its appeal. With that being said, however, I would not recommend it as a text for beginners by itself, as it tends to assume that the reader has already learned the basics set forth in the previous book. Taken as a companion volume, however, it does an excellent job of filling in the blanks with specific minutiae.

The best example of this sort of "in-depth" treatment is in Chapter 4, where Major spends fourteen pages (pp. 51-65) exploring the logical reasoning methods summarized in four pages in the earlier work. However, more than just providing a more detailed discussion of the issue, Major applies it in his trademark manner to specific examples, teaching by example as well as by rote. Another example is his expanded treatment of organizational aids (such as titles, headings, and sub-headings) and layout in Chapter 2, which were only discussed in broad terms in *Communicating with Intelligence.*

Perhaps the most important addition of this book, however, to the "Writing Guide" field is Chapter 3, entitled "What an Intelligence Analyst Does." This chapter is based on an article titled "Managing/Teaching New Analysts" written by Martin Petersen in 1985 for *Studies in Intelligence*, and reprinted in altered form in Major's 2004 JMIC text, *Style: Usage, Composition, and Form*, also reviewed herein. As an antecedent lecture to how intelligence analysts should write, this chapter first provides a primer on what intelligence analysis actually *is*, with the assumption that if writers know what their writing will be used for, they will be better able to tailor their writing to accomplish that goal. This chapter, the chapter in the 2004 JMIC book, and Petersen's original article (available at http://www.nationalsecuritylaw.org/files/received/CIA/Petersen-Managing_Teaching_New_Analysts.pdf) are all highly recommended reading for new analysts.

C. JMIC Press Works

Major wrote two style manuals for JMIC Press (now NDIC Press) before either of the above two SPIES volumes, and while the vast majority of the material included therein is duplicated in the later books, each of these JMIC texts does provide further detailed instructions that make them worth having on your bookshelf.

Style: Usage, Composition, and Form adds an in-depth discussion of how to write book reviews and annotated bibliographies (Chapter 5). As a subject near and dear to my heart, I strongly advise anyone wishing to submit a book review to *AIJ* or any other publication to review this chapter. Also, as mentioned above, Major's detailed treatment of the Petersen article in Appendix 3 is a must-read for novice intelligence analysts.

Citation: Note and Bibliographic Form adds specific instructions for citing sources that intelligence writers normally utilize that are foreign to most academic or journalistic writers, such as conference proceedings, briefings, government publications, and classified documents. If your written product must include such citations, this book will provide some much needed assistance in keeping them standardized.

II. USAGE GUIDES

Writing Classified and Unclassified Papers for National Security does double duty as a Writing Guide and a Usage Guide, and if an intelligence writer only had access to one Usage Guide in this review, this would be the text I would recommend. Specifically, Chapters 8 and 9 provide easily-accessible charts for such things as common abbreviations and problematic compound words, and Chapter 10 is nothing more than a usage glossary of terms common to intelligence analysis. However, each of the other reviewed texts does offer complementary coverage of such items.

Communicating with Intelligence, contrary to form, does in fact perform a more detailed treatment in Chapter 6 than *Writing Classified and Unclassified Papers for National Security* of one vital "usage issue," that of how to effectively use transitions to indicate how thoughts are related. This time, rather than limiting his discussion to big-picture items, Major spends some time detailing the different types of relationships that thoughts can have and specifying which transition terms are best suited for which relationships. The rest of the "usage material" of this book, however, is explored in greater detail in the later text.

The CIA's *Style Manual and Writers Guide for Intelligence Publications* is *solely* a glossary of terms (and occasionally rules) that by itself is quite limited in its usefulness except to writers who only need a reference text of that sort. Its organizational style is difficult to navigate and, for the rules that it proffers, Welch's *Analyst's Style Manual* (which is openly based on the "rules" portion of the CIA

guide) does a much better job of relaying the information. With respect to the terms listed, other guides handle this better, although the one redeeming factor of the CIA guide is the deadpan sense of humor that sometimes appears in unexpected places. Example A: "In CIA formal issuances, do not use the exclamation point." (p. 47) Example B: "Intelligence analysts, however, should *evaluate*, not feel." (p. 49) Example C: the mere fact that the author considered "dancercize," "karaoke," "willy-nilly," "worrywart," and my personal favorite, "stick-to-it-iveness," as words commonly misspelled by intelligence analysts. Given that this book appears to be out of print, its value to an intelligence writer is solely as a historical curiosity.

For the best glossary-style treatment of commonly problematic words, I recommend the NSA's *SIGINT Reporter's Style and Usage Manual*. While this manual also falls prey to the same flaw as the CIA guide of mixing rules and terms in an overall alphabetic structure, its value is not as a rule guide but as a glossary-style Usage Guide. In that capacity, it exceeds all expectations.

III. FINAL VERDICT

Communicating with Intelligence and *Writing Classified and Unclassified Papers for National Security* should together be among the most closely read books on any intelligence writer's bookshelf. However, novice intelligence writers are warned from using the latter without the former, as it takes for granted a certain level of foundational knowledge. Major's JMIC Press books should be used as reference guides for writers who need to write book reviews or annotated bibliographies (*Style: Usage, Composition, and Form*) and who need to cite sources of information not commonly described in the other style manuals (*Citation: Note and Bibliographic Form*). Neither the CIA's *Style Manual and Writers Guide for Intelligence Publications* nor the *Analyst's Style Manual* adds anything that is not present in the others but, if a reader must choose, the *Analyst's Style Manual* is a better source for rules than the CIA guide. For a sheer comprehensive glossary of commonly problematic terms, the best source by far is the NSA's *SIGINT Reporter's Style and Usage Manual*.

Notes

[1] The 6th edition reviewed herein is the most current publicly available edition. However, shortly after I wrote this review, I learned that a 7th edition, entitled *DI Style Manual for Intelligence Publications* and printed in 2004, does exist within the CIA for internal use. I have filed a Freedom of Information Act request for this edition, and when it is released I will make it available at http://www.nationalsecuritylaw.org/files/received/CIA/DI_Style_Manual.pdf.