

# AMERICAN INTELLIGENCE JOURNAL

*THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS*




*Intelligence Ethics and Leadership*

**NMIA**


---

Vol. 33, No. 1, 2016



***The United States finds itself in the most challenging strategic situation it has faced since the Cold War.***

—Ambassador Joseph DeTrani,  
President of the Daniel Morgan Academy



The Daniel Morgan Academy is a new graduate school whose mission is to educate the next generation of leaders to work the most difficult issues affecting the Nation. We provide a student-centric education for recent college graduates who desire to serve in the national security community. We also help mid-career professionals in credentialing their work experience or obtaining specialized knowledge for career advancement.

Visit ***DanielMorgan.academy*** to learn about our  
Master's and Graduate Certificate programs.



**DANIEL MORGAN ACADEMY**  
*A graduate school serving the national security community*

1620 L Street, NW, Seventh Floor, Washington, DC 20036  
202-759-4988 • [info@danielmorgan.academy](mailto:info@danielmorgan.academy)

**SERVE YOUR COUNTRY - SECURE YOUR FUTURE**

## NMIA Board of Directors

LTG (USA, Ret) James A. Williams, Chairman

Col (USAF, Ret) William Arnold, President

Mr. Louis Andre, Director

Col (USAF, Ret) Carla Bass, Director

Brig Gen (USAF, Ret) Scott Bethel, Director

Mr. Don Bolser, Director

CDR (USNR, Ret) Calland Carnes, Chapters Director

Col (USAF, Ret) John Clark, Director

Lt Gen (USAF, Ret) David Deptula, Director

LtCol James Eden, Director

Mr. Roland Fabia, Director

COL (USA, Ret) Michael Ferguson, Director

Mr. Terrance Ford, Director

Ms. Jane Flowers, Director

Col (USAFR, Ret) Michael Grebb, Treasurer

COL (USA, Ret) David Hale, Director

LTG (USA, Ret) Mary Legere, Director

Capt (USNR, Ret) Stephanie Leung, Director

Brad Moss, Esq., Director

Capt (USNR) Rick Myllenbeck, Director

COL (USA, Ret) Napoleon Stewart, Director

CDR (USNR) Louis Tucker, Director

COL (USA, Ret) Gerald York, Director

*Editor* - COL (USA, Ret) William C. Spracher, Ed.D.

*Production Manager* - Ms. Debra Hamby-Davis

LTG (USA, Ret) Harry E. Soyster, Director Emeritus

LTG (USA, Ret) Patrick M. Hughes, Director Emeritus

RADM (USN, Ret) Rose LeVitre, Director Emeritus

MG (USA, Ret) Barbara Fast, Director Emeritus

COL (USA, Ret) William Halpin, Director Emeritus

Dr. Forrest R. Frank, Director Emeritus

Mr. Antonio Delgado, Jr., Director Emeritus

Col (USAF, Ret) Joseph Keefe, President

Mrs. Zhi Ziegler, Director Emeritus

---

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 William Arnold (USAF, Ret). NMIA membership includes active duty, retired, 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 <[ajeditor@nmia.org](mailto:ajeditor@nmia.org)>. 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 welcomed. Questions concerning subscriptions, advertising, and distribution should be directed to the Production Manager at <[admin@nmia.org](mailto:admin@nmia.org)>.

The *American Intelligence Journal* is published semi-annually. Each issue runs 100-250 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.

Copyright NMIA. Reprint and copying by permission only.

**Accenture**

**Allied Associates International, Inc.**

**American Military University**

**ANSER, Analytic Services, Inc.**

**CACI**

**CGI**

**Daniel Morgan Academy**

**Digital Globe**

**DynCorp International**

**General Dynamics Advanced Information Systems**

**General Dynamics Information Technology**

**Kiernan Group Holdings**

**Leidos**

**MDA Information Systems, LLC**

**Northrop Grumman Information Systems**

**PARSONS**

**Pluribus International Corporation**

**Riverside Research Institute**

**SOS International, Ltd.**

**SYTERA, LLC**

---

**NMIA gratefully acknowledges the generous support of Daniel Morgan Academy in Washington, DC. DMA has sponsored the publication of this Journal, including distribution assistance for its delivery into the IC.**

---

## Table of Contents

President's Message .....	1
Editor's Desk .....	2
Leading and Managing Intelligence Organizations by Peter C. Oleson and RADM (USN, Ret) Tony L. Cothron .....	6
Activity-Based Intelligence: Coping with the "Unknown Unknowns" in Complex and Chaotic Environments by Col (USAF) James L. Lawrence II .....	17
Is Intelligence an Instrument of National Power? by Dr. Adrian Wolfberg and CDR (USN) Brian A. Young .....	26
North Korea's Post-Totalitarian State: The Rise of the Suryong (Supreme Leader) and the Transfer of Charismatic Leadership by Dr. David W. Shin .....	31
The Moral-Ethical Domain and the Intelligence Practitioner by LTC (USAR, Ret) Christopher E. Bailey .....	49
The Big Brother Fear: Four Perspectives on Surveillance by Dimitrina Galantou .....	59
Hegelian Dialectics as a Source of Inspiration for the Intelligence Community by Dr. Pelle de Meij .....	65
The Road to High-Quality Decision-Making: Understanding Cognition and the Phenomenon of Groupthink by Troy E. Smith .....	70
Demographics and Conflict by Dr. Michael M. Andregg .....	74
Lanes in the Road: Streamlining Intelligence Community Congestion by LTC (USA, Ret) Thomas M. Cooke .....	79
The Future of the American Intelligence Establishment by Dr. William E. Kelly .....	88
A Conspiracy Against the Laity: Does the Intelligence Community Need an Ethical Code to Become Truly a "Profession"? by Erik D. Jens .....	92
Mired in Gray: Juggling Legality, Lawfulness, and Ethics as an Intelligence Professional by Dr. William C. Spracher .....	96
Intelligence Analysts: Continuing Education for Enduring Strategic Value by LTC (USA) Joseph D. Becker .....	104



# AMERICAN INTELLIGENCE JOURNAL

---

## Table of Contents (*Continued*)

In My View...

Lessons on Cyber Security: A NASA Case Study by Dr. Joshua Tallis .....	109
--	-----

Profiles in Intelligence series...

Can Traits of a Successful Military Commander Be Those of a Good Intelligence Director? by Dr. Kenneth J. Campbell .....	111
---	-----

NMIA Bookshelf

Douglas Waller's <i>Disciples: The World War II Missions of the CIA Directors Who Fought for Will Bill Donovan</i> reviewed by John R. Clark .....	121
---	-----

Michael V. Hayden's <i>Playing to the Edge: American Intelligence in the Age of Terror</i> reviewed by Dr. Edward M. Roche .....	122
---	-----

Michael T. Flynn and Michael Ledeen's <i>The Field of Fight: How We Can Win the Global War Against Radical Islam and Its Allies</i> reviewed by Dr. George W. Ridge .....	123
--	-----

William M. LeoGrande and Peter Kornbluh's <i>Back Channel to Cuba: The Hidden History of Negotiations between Washington and Havana</i> reviewed by Jaime Gonzalez and Dr. David R. Lessard .....	124
--	-----

Jonathan S. Lockwood's <i>The Lockwood Analytical Method for Prediction (LAMP): A Method for Predictive Intelligence Analysis</i> reviewed by Dr. John Sislin .....	126
--	-----

Peter Caddick-Adams' <i>Monte Cassino: Ten Armies in Hell</i> reviewed by Harry L. Petrey II .....	129
---	-----

Review essay on three books dealing with captured U.S. intelligence collection vessels, titled "Spy Ships and the Collection of Signals Intelligence": A. Jay Cristol's <i>The Liberty Incident Revealed: The Definitive Account of the 1967 Israeli Attack on the U.S. Navy Spy Ship</i> , Jack Cheevers' <i>Act of War: Lyndon Johnson, North Korea, and the Capture of the Spy Ship Pueblo</i> , and Mitchell B. Lerner's <i>The Pueblo Incident: A Spy Ship and the Failure of American Foreign Policy</i> by LTC (USAR, Ret) Christopher E. Bailey .....	131
--	-----

***The opinions expressed in these articles are those of the authors alone. They do not reflect the official position of the U.S. government, nor that of the National Military Intelligence Association, nor that of the organizations where the authors are employed.***

## President's Message

---

I know that there has not been a “President’s Message” included in the last several editions of *American Intelligence Journal*. Therefore, I will use this space to catch NMIA members up on a number of issues.

First, I should introduce myself and explain the circumstances surrounding my assumption of the office of President. My name is Bill Arnold and I have been on the NMIA Board of Directors for approximately 15 years. I was previously the Association’s Secretary and before that directed the NMIA and National Military Intelligence Foundation (NMIF) Awards Program for four years. I am a retired Air Force colonel, having spent my career with the Office of Special Investigations and a good deal of that time in the counterintelligence discipline. My last active duty assignment was on the U.S. European Command J2 staff. Following my retirement from the Air Force, I worked for various government contracting companies primarily supporting intelligence and counterintelligence programs.

I recently took over as President from Joe Keefe who held that position for eight years. Unfortunately, Joe stepped down from the position for medical reasons. For those of you who know Joe, he is doing well now and looks forward to a complete recovery.

Second, I pledge my complete support to NMIA and its goals. In sum, the NMIA leadership is dedicated to “giving back” to the military intelligence communities by developing products and programs aimed at enhancing the professional development of current practitioners of all the military intelligence disciplines. In pursuing this goal, we need help from each NMIA member in providing suggestions for how we can improve our products and programs. If any of you have ideas for enhancing our products or symposia or, in any other way, improving our support to you, our customer, please make these known to us via [admin@nmia.org](mailto:admin@nmia.org).

Third, we need your help in spreading the word on the value of NMIA membership. To be honest, we have seen a drop in the number of NMIA individual and corporate members over the past three years. We suspect the drop in corporate membership is at least in part connected with the reaction of the defense contracting community to sequestration. Here again, any suggestions you may have regarding actions we can take to increase our individual and corporate membership would be greatly appreciated.

I look forward to working with you over the coming months and hope to have an opportunity to meet you in person at one of our upcoming events.

William R. Arnold  
President



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

**Submit a manuscript for  
consideration  
to the Editor <[ajeditor@nmia.org](mailto:ajeditor@nmia.org)>**

## The Editor's Desk

---

Greetings from our Nation's Capital in the midst of a wild and wooly presidential election year! What better time could there be for the *American Intelligence Journal* to adopt a theme dealing with leadership? Actually, the theme is "Intelligence Ethics and Leadership," and we have some outstanding contributions by authors from both inside and outside the Intelligence Community.

The institution where we teach, the National Intelligence University, decided to make "Leadership" its central focus for 2015. The former Director of the National Geospatial-Intelligence Agency, Letitia "Tish" Long, keynoted the annual NIU Convocation ceremony welcoming new students with an address on the subject. A couple weeks later, the inaugural speaker for the weekly NIU President's Lecture Series was Principal Deputy Director of National Intelligence Stephanie O'Sullivan, who also stressed the importance of intelligence leadership. NIU had just kicked off a new certificate program in "Leadership and Management in the Intelligence Community," later introduced an academic concentration by the same rubric, established a new core course in its two master's programs (which we have been privileged to teach), and then created a new academic department, Intelligence Enterprise, to support the teaching of leadership and management-related courses. Heretofore, leadership, management, and ethics had received only scattered attention at NIU through occasional electives often taught by adjuncts who tended to be retired IC practitioners. The newfound emphasis on leadership and ethics was a conscious and deliberate attempt to raise the subject to the level of emphasis it deserves.

NIU's parent agency, DIA, likewise has jumped on the leadership bandwagon. A year into his tenure as Director, in February 2016 LtGen (USMC) Vince Stewart announced his five specific priorities for 2016, and #1 on the list was "developing our leadership." The other four included strengthening education and training (the theme for *AIJ*, Vol. 31, No. 2, 2013), improving content delivery, modernizing the human resources IT system, and furthering integration across the intelligence enterprise. Intelligence integration has been a particular emphasis of the DNI, Jim Clapper, ever since he assumed that position six years ago after previously holding such key leadership posts as both DIA and NGA Director and Under Secretary of Defense for Intelligence.

Ethics goes hand in hand with leadership. Director Clapper has promulgated a code of ethics for the entire IC, based in part on the separate codes of ethics of the individual agencies already in place and in part on an intriguing initiative in which he asked graduate students at NIU to formulate a draft code for his consideration. Some of the instructors teaching courses on ethics, the rule of law, and leadership—who oversaw this critical work in 2012 by their students—are represented in the pages of this edition of *AIJ*. We were both fortunate to be able to sit in when several NIU students presented their findings to the DIA and ODNI leadership. This is a perfect example of how academics can be used to bridge the gap between theory and practice. In fact, DNI Clapper opened his 2014 National Intelligence Strategy (NIS) with the "Principles of Professional Ethics for the IC," remarking that "it is nonetheless important for the Intelligence Community to set forth in a single statement the fundamental ethical principles that unite us and distinguish us as intelligence professionals."

The IC recently has been faced with a number of dilemmas related to ethics in intelligence analysis and reporting, such as the alleged manipulation of intelligence by officials at U.S. Central Command regarding how the wars in Syria and Iraq are going. Specifically, whistleblower-type reports began emerging in late 2015 that CENTCOM analysts' work was being altered to show more progress against the Islamic State than had actually been achieved. A Congressional Task Force on CENTCOM released its initial report on August 11, 2016, detailing persistent problems in 2014 and 2015 with the command's analysis of U.S. efforts to train Iraqi security forces and combat the so-called Islamic State in Iraq and Syria. The TF found that "intelligence products approved by CENTCOM leaders typically provided a more positive depiction of U.S. anti-terrorism efforts than analysis produced by other elements of the Intelligence Community." It further determined that "numerous process changes implemented at CENTCOM as well as leadership deficiencies resulted in widespread dissatisfaction among CENTCOM analysts who felt their superiors were distorting their products." The TF was established by the chairmen of the House Armed Services Committee, the House Permanent Select Committee on Intelligence, and the Subcommittee on Defense of the House Appropriations Committee. The TF's work is still ongoing, occurring alongside a separate investigation by the DoD Inspector General. Clearly, the conduct and ethics of intelligence leaders are at the heart of this key inquiry.



Of course, this is not the first time intelligence has been “politicized” and it certainly will not be the last. We tell our students that politicization in the intelligence business is unavoidable but nevertheless must be minimized and contained. The IC continues to recover from the faulty National Intelligence Estimate on Iraqi weapons of mass destruction that helped lead the U.S. to war in 2003. Analytical improvements have been made since then, but unless intelligence officials adhere to high ethical standards and try to avoid politics—while still informing policymakers of the real threat to the best of their ability—controversial problems will arise. In July 2016, the former Chairman of the Joint Chiefs of Staff, GEN (USA, Ret) Martin Dempsey, wrote a letter to the editor of *The Washington Post* lamenting that two of his former colleagues—Gen (USMC, Ret) John Allen and LTG (USA, Ret) Michael Flynn—had stooped to the level of endorsing presidential candidates and giving partisan speeches at the two national conventions. The recently retired CJCS asserted that “the military is not a political prize. Politicians should take the advice of senior military leaders but keep them off the stage.” On this score, GEN Dempsey is on the mark.

In this issue of the *Journal*, the leadoff article is by two veterans of the IC and former senior leaders, Peter Oleson, a former DIA official and UMUC professor now on the board of directors of AFIO (Association of Former Intelligence Officers), and RADM (USN, Ret) Tony Cothron, former Director of Naval Intelligence and a former member of the NMIA board. They discuss many of the principles of leadership and management and how the two fields differ, quoting such scholars as Joseph Nye, Peter Northouse, John Kotter, and James McGregor Burns and applying their theories to challenges faced by the IC in the 21<sup>st</sup> century. They also lean on the wisdom of such astute leaders as ADM (USN, Ret) Bill Studeman and GEN (USA, Ret) Stan McChrystal. Col (USAF) James Lawrence’s article is based on a professional studies paper he wrote for the Air War College. He discusses the growth of the ISR enterprise, which is complicating processes and methodologies employed to produce finished intelligence, and the flood of data that is making analysis more difficult. He adds that the counterinsurgency campaign in Afghanistan has set the stage for a transformation in analytical methodology to address complex and chaotic problem sets. Lawrence argues for adoption of an activity-based intelligence (ABI) methodology, an appropriate follow-on to one of the 2015 issues of *AIJ* that explored the theme “New Paradigms of Intelligence Analysis.” Adrian “Zeke” Wolfberg and CDR (USN) Brian Young of the Army War College assess the role of intelligence in the realm of strategic thinking and ask whether intelligence is an instrument of national power or merely an enabler of it. Zeke is the DIA Chair at the College and formerly headed a knowledge management entity at DIA. They argue that a political problem exists when we

want intelligence to be an instrument because we misunderstand its nature and diminish its ability to speak truth to power. The authors insist there is a risk by absorbing intelligence into the policymaking arena, which reminds me of the famous Kent-Kendall debates of the 1940s/50s regarding the proper place of intelligence in strategic decision-making and where the line should be drawn as analysts offer advice to policymakers.

COL (USA, Ret) David Shin of NIU examines the often explosive leadership of North Korea in an article based on his recent doctoral dissertation, which explored the perpetuation of an autocratic regime through the application of Nye’s concept of “smart power” (the mix of hard and soft power). Shin argues that the first two generations of the Kims were both capable and charismatic leaders, while the third Kim (Jong-un) is trying to follow their lead to demonstrate his competence and potential as the new Supreme Leader. This flies in the face of the commonly held opinion that all three Kims were nothing more than bizarre, thuggish, out-of-control dictators who care nothing for the human rights of their citizens. Dave lays out the case that the Kims have adroitly based their legitimacy on refining their historical legacy, invoking the leadership theories of Northouse, Burns, and Nye. Thomas Cooke’s article reviews the historical changes and reforms in the U.S. IC due to changes in the threat, resource availability, and the increasing number of players in the Community, causing congestion and too much redundancy/duplication of effort. Tom goes back to the basics by focusing on the enemy’s capability and intent, arguing that agencies should concentrate on their formal functional management responsibilities. Leaders are striving for relevance and to have their voices heard, but this causes unnecessary redundancies that the IC can no longer afford.

NIU faculty member and legal scholar LTC (USAR, Ret) Christopher Bailey has contributed a salient piece on “The Moral-Ethical Domain and the Intelligence Practitioner.” Chris argues that the principles of ethics promulgated in the 2014 NIS provide a useful starting point for intelligence practitioners, but also obscure some important issues, such as the nature of the client relationship, standards of practice, and professional relationships among practitioners. Moreover, he insists that the principles do not address other issues practitioners face. The interesting point here is that Chris was actually one of the primary organizers for NIU’s 2012 ethics conference which later led to the principles promulgated by the DNI! In any case, this article is actually a companion piece to a 2013 article he published in the *International Journal of Intelligence Ethics*, “The Intelligence Community Ethos: A Closely Regulated Profession.”

This issue, as usual, boasts a handful of international authors. First we have Dimitrina Galantonu of Romania, which has become a big player in NATO and European Union intelligence circles. Dimitrina came to the National Defense University at Fort McNair during academic year 2015-16 from the Romanian National Intelligence Academy in Bucharest, where she has been a PhD candidate. This young Fulbright Scholar looks at mass government surveillance in an increasingly interconnected electronic world, and how human beings view the tradeoff between civil liberties/privacy and security. She examines what she calls “attribution theory” and discusses modern challenges in terms of ethicists and philosophers like Baruch Spinoza, Karl Popper, and Benjamin Franklin, and what they might think of the “big data” concerns of today. She concludes it all boils down to the human mindset and what causes the most fear, and that fear can be overcome by increased knowledge. There have been quite a few Romanian scholars in recent years at conferences hosted by such organizations as the International Studies Association (ISA) and International Association for Intelligence Education (IAFIE), and I am pleased that several have contributed articles to *AIJ*. Next, Pelle de Meij of the Netherlands looks at Hegelian dialectics (Georg Wilhelm Friedrich Hegel was a noted German philosopher) and argues that ethics should inspire the intelligence enterprise. He contends the IC is the ultimate guardian of the rule of law, democracy, and human rights, and compares Hegel’s views to those of Immanuel Kant, Karl Marx, and Friedrich Engels. To accomplish this role, there is a need for structured oversight and control mechanisms for the intelligence services, such as inspectors general, general counsels, entities such as the Office of Management and Budget in the U.S., and legislative committees. The author talks about the principles of ethical conduct for government officials and offers the global IC the same set of fundamental ethical principles that distinguish intelligence professionals—mission, truth, lawfulness, integrity, stewardship, excellence, and diversity—laid out by DNI Clapper two years ago. Our final international author in this issue is a repeat contributor several times over to the pages of the *Journal*, Troy Smith of Trinidad and Tobago. He discusses how national strategy directs leaders in making policy and dealing with its many political ramifications. Troy also explains how the decision-making process from which strategy emerges must cope with cognitive errors and groupthink.

An ethics scholar whom we first met over a decade ago through organizations such as the International Intelligence Ethics Association (IIEA) and ISA’s Intelligence Studies Section, Michael Andregg, contributes his second article to *AIJ*. Dr. Andregg is a civilian professor who researches the ethics of wargaming

and peacekeeping, and in this piece explores the importance of demographics, or the characteristics of populations, in causing instability. We have all heard about chaotic nations with exceedingly young populations and a “youth bulge” which, when associated with high unemployment and a weak economy, can be explosive. Most of the IC’s time is spent watching emerging threats in such unstable parts of the world, where “failing states” compete with already “failed states” for the attention of decision-makers trying to avoid deleterious spillover effects and the spread of terrorism. Erik Jens, another frequent contributor to *AIJ*, is a lawyer who teaches courses on ethics and legal issues at NIU. He piggybacks onto a long-standing debate in the U.S. over whether intelligence is truly a profession, like medicine and the law. After ticking off a list of indicators/standards, he concludes that it is not, though within the IC the analysts and collectors come closest to qualifying. Erik suggests that subsets or “tribes” of the IC qualify to a degree but not the Community as a whole. He insists it is more useful to view it as a “community of professionals.” This of course differs from the earlier views of Director Clapper, as spelled out in his 2014 NIS: “We assess that ‘intelligence’ qualifies as a profession, because we in the IC have unique access and training, so we’re capable of reaching informed decision when the general public can’t, and that’s true across the IC.” Yet another repeat contributor to *AIJ* is LTC (USA) Joseph Becker, now with ODNI and formerly on the NIU faculty. In an IAFIE award-winning essay, Joe argues that in an era of increasing technical capability the focus is on the modes of collection and tools of analysis, rather than on the capacity of the analysts themselves, creating the perception of a diminished role for individual analysts. He examines the role and function of the analyst and his/her importance to the overall intelligence system. He also insists the IC must develop its strategic thinkers by placing a higher priority on continuing education, based on the application of theory. Joe rues the fact that training is considered a necessity but education is not.

Due to a dearth of manuscripts submitted for this issue specifically dealing with ethics, though that field and leadership are inexorably intertwined, the editor-in-chief decided to resurrect an article he first wrote while a graduate student back in the late 1970s but whose enduring lessons are still applicable today. It assesses how intelligence operations can be viewed through various lenses—their legality, lawfulness, and effectiveness. A revised/updated version of the piece was first published in *AIJ* in 2007 and is reprinted here.

The *Journal's* aperiodic opinion section "In My View" offers an article by Joshua Tallis, which can be viewed as a preview of an upcoming issue in 2017 that will examine "Cyber Threats" and follows up an issue we produced in 2011 on "Cyber Security and Operations." Just like we try to include at least one article on China in each issue (we failed this time around, but North Korea is a Chinese client state!), cyber has become so important of late there has been an article or two on cyber in each issue. This short essay was written as a think-piece—hence placed in this section—as it takes a seemingly unrelated incident, the 2003 break-up of the Space Shuttle Columbia, and demonstrates how lessons learned from that tragedy should be applied to dealing with the creeping, silent cyber threat of today. Alarm bells should be going off but, according to Josh, the anonymous, remote nature of the threat is often misdiagnosed and underappreciated. Another special section is "Profiles in Intelligence," more often than not the private preserve of Dr. Ken Campbell, a prolific historian who has provided so many stimulating articles in the past, most of them about World War II intelligence heroes and villains. In his latest contribution, ideally suited to our leadership theme, Ken examines whether the traits of a successful military commander parallel those of a good intelligence director. He does this through a profile of Wolfram von Richthofen (no, not Manfred von Richthofen, the "Red Baron" of World War I flying ace fame and Wolfram's cousin!).

A couple of the book reviews in this edition fit our leadership theme nicely, especially Doug Wallers' book about the "Disciples" of OSS chief "Wild Bill" Donovan who later became DCIs themselves, and Gen (USAF, Ret) Michael Hayden's book about "playing to the edge" in an age of terror. The latter was the motive for an informative and inspirational presentation and book-signing by Hayden in August 2016 in Alexandria, VA, sponsored by NMIA and its NCR Chapter. Jonathan Lockwood's book outlining his "analytical method for prediction" (LAMP) probably would have better complemented the 2015 issue on analysis. Still, leaders and managers of intelligence would do well to heed Lockwood's commonsense advice about the use of analytical techniques. Similarly, operational intelligence leaders need to review the history of U.S. collection platforms that were compromised, as laid out in an incisive review essay by our guest co-editor for this issue, LTC (USAR, Ret) Christopher Bailey. The editor-in-chief asked Chris, who has often contributed both book reviews and feature articles to *AIJ* in the past, to backstop him for this issue given his rare expertise. A legal scholar and attorney, Chris has taught courses at NIU dealing with ethics and national security law. He proved invaluable in reviewing the offerings in this issue and sagely commenting on them.

Finally, here is the roadmap of our way ahead for the next three issues of the *Journal*:

Vol. 33, No. 2, 2016: "Intelligence in Peace and War" (already closed out; manuscripts were due by October 31, 2016)

Vol. 34, No. 1, 2017: "Cyber Threats: The Future of Intelligence in a Wired World" (inputs must be submitted by April 30, 2017)

Vol. 34, No. 2, 2017: "Honoring our Intelligence Heroes: The Historical Heritage of NMIA/NMIF Awards" (inputs must be submitted by October 31, 2017)

We urge you to reach out to the editor-in-chief at his *AIJ* editor's address posted on these pages or his NIU address at [William.Spracher@dodis.mil](mailto:William.Spracher@dodis.mil) if you would like to contribute an article or book review, whether it fits closely with one of the announced themes or not. We at NMIA value your support and feedback!

*Bill Spracher*  
*Chris Bailey*

[Editor's Note regarding Vol. 32, No. 2, 2015: One of the articles reprinted from an older journal, "Hiding in Plain Sight," inadvertently included an outdated bio for the author. Here is the updated version: R. Kent Tiernan, now retired from the Senior National Intelligence Service (SNIS), is former Staff Director and Vice Chairman of the Foreign Denial and Deception Committee of the National Intelligence Council (NIC). He has been involved with various aspects of deception for over 30 years as Air Force Special Studies Division Chief, a U.S. government contractor, and an SNIS for the NIC. He received a BA in History from Stanford University and an MA in Western European Area Studies from the University of Notre Dame.]

Bill Spracher, Editor



---

# Leading and Managing Intelligence Organizations

by Peter C. Oleson and RADM (USN, Ret) Tony Cothron

---

**I**ntelligence, in living organisms and in any human organization, is defined as the ability to perceive information, retain that information as knowledge, and then apply that knowledge for a task or purpose. In this article our focus is on the special and unique characteristics of leading and managing an intelligence organization, both large and small.

There is a large body of knowledge, education, and training on leadership and on management, and all can benefit from a lifelong commitment to studying and improving upon their own personal capabilities in this area. It is our belief that the art of leadership and management required for intelligence leaders is a subject of special importance. Not only must intelligence leaders provide timely, relevant, and predictive intelligence to support decisions that literally have life and death results, they must navigate and manage the incredible complexity of U.S. and international laws, global technology, interagency politics, an evolving workforce and, lest we forget, dynamic threats.

Once the exclusive purview of the nation-state, intelligence is now employed by many constituencies such as:

- National Intelligence Community (including the Director of National Intelligence (DNI), the Central Intelligence Agency (CIA), the elements of intelligence in the Defense Department, including the military services, and in other Cabinet-level departments);
- Homeland security community (including the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI) and its Joint Terrorism Task Forces (JTTF), and state-level law enforcement and fusion centers);
- Law enforcement agencies at the federal, state, local, and tribal levels; and
- Private sector corporations.

Intelligence has no intrinsic value. Intelligence collected, analyzed, and put on the shelf is worthless. It is wasteful of expensive and often dangerous efforts. Intelligence is a service, and should be evaluated as such. Its *raison d'être* is to assist others in the accomplishment of their goals.

Intelligence, in any organization, is a specialized function that adds value by providing decision advantage to leaders and members of the organization. In some cases, this value may be in increased efficiency, but most often it is because of increased effectiveness. To have any success or positive effect, the leader and manager of an intelligence function must ensure a focus by all personnel and resources on supporting the decision-maker's needs. Chairman of the Joint Chiefs of Staff Colin Powell reportedly explained to his Director of Intelligence: Tell me what you know, what you don't know, and what you think, but make sure you differentiate between each.

## WHAT IS LEADERSHIP?<sup>1</sup>

**H**ow is leadership different from management? "...[L]eadership remains an ambiguous, amorphous, and frequently misunderstood concept."<sup>2</sup> It is "...one of the most observed and least understood phenomena on earth."<sup>3</sup> "One of the major problems in understanding leadership is that 'leadership' is often confused with 'management' to the detriment of both."<sup>4</sup>

Leadership is different from management. Rather, leadership and management are two distinctive and complementary systems of action. Each has its own function and characteristic activities. Both are necessary for success...<sup>5</sup>

There are many clichés about leadership; some are enlightening:

- "You manage things; you lead people."  
— Grace Hopper (RADM, USN, Ret), computer pioneer.
- "The manager focuses on systems and structure; the leader focuses on people."  
— Warren Bennis, University Professor and Distinguished Professor of Business Administration and Founding Chairman of the Leadership Institute at the University of Southern California.
- "A much quoted bromide...defines 'management' as the skill of getting people to do something that you want them to do because you want them to do it and 'leadership' as the



---

art of getting people to do something you want them to do because they want to do it.”  
—Sal F. Marino, media CEO in “The Difference between Managing and Leading,” *Industry Week*, June 17, 1999.

To support his leadership course, Harvard Professor Joseph S. Nye wrote about the array of powers available to any leader:

- Coercive power, which is “based on fear and relates primarily to the ability of the leader to punish the subordinates for non-conformity.”
- Reward power, which “relates to the ability of the leader to provide positive rewards, such as income or other benefits, to people who cooperate.”
- Legitimate power, which “relates to the position of the leader in the organizational hierarchy.”
- Expert power, based on “unique expertise or skills in particular areas that are regarded as important to subordinates.”
- Referent power, “essentially the power of personality and relates to the leader’s ability to be admired because of one or more personal traits.”<sup>6</sup>

Nye calls the first three powers “hard power” and the second two “soft power.” Many authorities on leadership believe that the power position of the leader with regard to subordinates is a critical factor in determining leader effectiveness. Thus, while acknowledging that today, especially in the governmental bureaucracy, it is preferable to use soft power, Nye recognized that to lead effectively leaders often need to use a combination of both hard and soft power. He termed this “smart power.”

Nye states that “you cannot lead if you do not have power,” and that “...leadership and power are inextricably intertwined.” “Leadership is a power relationship between leaders and followers....” Nevertheless, a caution! Long ago Aristotle noted “leadership involves power, but not all power relationships are instances of leadership.” In other words: Do not confuse leadership with power. Leadership gives power but power does not bring leadership.<sup>7</sup>

John W. Gardner, former Secretary of Health and Human Services, founder of Common Cause, and president of the Carnegie Foundation, has pointed out:

One reason corporate and governmental bureaucracies stagnate is the assumption by line executives that, given their rank and authority, they can lead without being leaders. They cannot. They can be given subordinates, but they cannot be given a following. A following must be earned. Surprisingly, many of

them do not even know that they are not leading. They mistake the exercise of authority for leadership, and as long as they persist in that mistake they will never learn the art of turning subordinates into followers.<sup>8</sup>

In management philosophy the ethical dimension of leadership today receives strong emphasis. What appears to be evolving is a philosophy that integrates performance, leadership, and ethics into a single construct, called performance ethics. There can be no doubt that the elements of leadership, ethics, and performance will increasingly be a part of intelligence management. Collectively, performance ethics demands results driven by committed leaders who are focused on achieving objectives in support of the public interest.

Performance ethics requires that all government leaders meet the following five leadership standards:

- Engage in debate that centers on the right course of action, not the most expedient, self-serving, or politically correct actions;
- Have the wisdom and courage to speak truth to power, to be candid in identifying unaddressed risks and their potential consequences, and in identifying the critical issues and obstacles that limit progress and permit vulnerabilities and liabilities to continue;
- Commit personally to see projects through, to ensure aggressive action, and to personally ensure that such action is sustained over time;
- Accept personal responsibility for results and activities conducted in support of those results; provide the organization with sufficient confidence to encourage risk-taking and innovation; and
- Create and maintain an organizational culture reflective of mutual trust; inspire the workforce and encourage its full commitment to the leadership agenda.

The performance ethics framework reflects the attributes of real leaders who have led committed people toward successful performance in real organizations.

Leaders must shape an organization and be responsible and accountable; they must manage the work and output of an organization. Keeping this in mind, the table on the next page compares the different sets of tasks that a leader and manager must simultaneously accomplish, whether that person is the head of a large organization or only a small element within a larger command or agency.



LEADER'S CONCERNS	MANAGER'S FOCUS
Ascertaining what the organization's mission is. How should it evolve?	Providing the most effective and efficient mission support.
Attracting, training, and retaining the highest quality personnel.	Managing personnel assignments for the best mission support.
Promoting teamwork, collaboration, and an ethical environment.	Improving the organization, its processes, and its standard operating procedures.
Mastering technology now and in the future.	Measuring performance and effectiveness.
Emphasizing safety and security.	Ensuring legal and ethical behavior.

Leadership of an intelligence organization takes a special focus, time, and forethought to stay ahead of policy and operational demands. Given the time and resource requirements to collect, process, analyze, and then disseminate intelligence to leaders, planners, and operational personnel, the intelligence leader must anticipate the need and have deep insight into the capacity of his organization to adapt to new tasking and to deliver, on time, new intelligence, while still working on existing tasks. The former acting Director of Central Intelligence, Admiral (USN, Ret) William O. Studeman, wrote that leadership requires seniors "getting their heads out of their schedules and in-baskets, and driving their organizations to the highest level of performance based on strategy, direction, vision, objectives, and goals."<sup>9</sup> Large organizations are highly resistant to change, especially lacking an actual external, crisis event (e.g., a 9/11-type attack), and effective intelligence leaders both recognize the need to transition to new tasks ahead of the demand and are successful in motivating the organization to change. An important element of the intelligence leader's role is also deciding, after changing tasking, which old tasks cannot be completed and conveying that risk to superiors.

### Management of Intelligence

Whether one defines intelligence as knowledge, a process, a product, an organization, or an activity, management of intelligence is similar to management in other fields. A manager sets out to accomplish his goals by orchestrating the resources he/she has available. These include financial and physical resources as well as human resources. The basic functions of management are well documented and include:

- Planning. This includes determining the vision and identifying the functions of the organization (the *what*) and planning how they will be performed (the *how*). Included are also the *where*

and *when* of the organization's activities. At more senior levels of management, planning for the resources and manpower needed to accomplish the functions of the organization is a major responsibility (the *wherewithal*).

- Organizing. This involves establishing the structure of the organization and who does what, including the boundaries of responsibilities and procedures.
- Directing. This involves guiding (and in some cases steering) the organization's collaborative activities through communication and development of policies and guidelines.
- Controlling. The mechanisms for a manager to control organizational activities involve oversight, feedback, and evaluation.<sup>10</sup>

Thomas Edison has been quoted as saying that "leadership without execution is hallucination." Within an organization, execution must be led and managed. One model that incorporates the role of leadership and management and used by one of the authors in leading large intelligence organizations is reflected in the figure below. The four quadrants represent all the elements of a typical organization with the circle representing the mission. The leader's key role is to set the vision, the direction for the organization and then manage and align each of the quadrants toward that vision. The utility of this model is in reminding the leader not to fall into the trap of focusing just on the organizational diagram and people. The capacity of the organization for output is reflected in the bottom two quadrants. Process is how work actually gets done and Culture is best understood as the sum of "Standard Operating Procedures" carried out over time. Any leader announcing or intending to "change the culture," and who does not cause activities to change, is not affecting the culture of an organization. Process and Culture are at the core of how any organization works and what it believes in, and these change only over time.

For intelligence leaders, the dynamics of new threats, new technology, new collection sources, “big data,” and the new tools of advanced information technology, as well as the ever-changing needs of decision-makers, all result in the need for frequently adjusting course and paying close attention to all four quadrants of the organization to ensure success.

## A Leadership Model

Taking a Comprehensive View



Source: US Naval War College

## THE FOUR FUNCTIONS OF INTELLIGENCE MANAGEMENT

Leadership without management will fail. Management without leadership is also unlikely to succeed. The four fundamental functions of management (planning, organizing, directing, and controlling) are both sequential and looped; that is, controlling—which involves feedback mechanisms—should influence subsequent planning for change, as necessary.

### 1. Planning for Intelligence

Planning has many aspects. It can also be the most complex and difficult of management functions because of its multiple parameters.

While planning is the initial managerial function to be accomplished, a manager at any level in an organization must know where he/she (henceforth, we shall use “he” for simplicity) is headed in order to plan effectively. Based on a vision, he must know his mission and his goals. From those he develops a strategy. The focus on strategy must be not on the goals, but on understanding available resources and

determining how they can best be used to meet the goals. The best way to look at strategy is to use the definition “Ends, Means, and Way” where ends are the goals, means are the resource, and way is what you do with what you have. The most successful organizations focus on and adjust what they are doing with what they have and with a constant focus on goals.

In his course on intelligence leadership, Professor Manthorpe addresses the importance of leadership and management in this context.

Accomplishing or achieving “goals” means something beyond accomplishing the daily mission. Goals are where the organization or people want to be or what they want to be doing in the future. The goals are set well in advance. For example, in the Intelligence Community, goals must be set to guide the planning, programming, and budgeting process, which has a 2- to 5-year lead time. The military planning process is likewise long-term. Goals imply aspiring to something beyond that which now exists—i.e., preparing the organization to accomplish the mission against new challenges in a way that is different or better than that which is being done now. Consequently, to achieve goals means leading change. Leaders must recognize the need for change and lead people to accept the need to change and bring change to the organization.

Change is hard but not impossible to accomplish. To lead change successfully a leader should recognize that, although it is a common belief, it is not true that people hate change and always resist it. By way of example, consider how Americans have all accepted and adopted great changes in technology. We have done so because those changes have brought us the benefits of making our lives more secure and our daily lives easier or better, and we have been able to accommodate those changes on our own terms and schedule and with fairly good certainty that once we buy the product we can get it to work. Thus, people actually:

- Just hate and resist change when they do not know what the outcome will be.
- Just hate and resist change imposed from above.
- Just hate change that brings them no benefits.
- Just hate and resist drastic, rapid change.
- Just hate and resist change that seems to be change for change sake.

---

Machiavelli advised the leaders of his day in *The Prince*, writing:

It must be considered that there is nothing more difficult to carry out, nor more doubtful of success, nor more dangerous to handle, than to initiate a new order of things. For the reformer has enemies in all those who profit by the old order, and only lukewarm defenders in those who would profit by the new order, this lukewarmness arising partly . . . from the incredulity of mankind, who do not truly believe in anything until they have had actual experience from it.

Ron Heifitz and Lawrence Lindsey have warned leaders of today:

To lead is to live dangerously because when leadership counts, when you lead people through difficult change, you challenge what people hold dear—their daily habits, tools, loyalties and ways of thinking—with nothing more to offer perhaps than a possibility. People push back when you disturb the personal and institutionalized equilibrium they know. And people resist in all kinds of creative and unexpected ways that can get you taken out of the game, pushed aside, undermined or eliminated.<sup>11</sup>

Hence, the initial step of planning is a challenging one.

Vision and Mission Statements. The critical first step in planning is the determination and articulation of a vision. Without this, it is impossible to communicate to managers or subordinates what the overarching goals of the organization are. This is a challenge at all organizational levels. General James L. Jones (USMC, Ret) has stated that it is important to convince your subordinates that your vision is their vision. That means giving them a stake, creating “buy-in” so they also have personal ownership of the policy. This was how to get results without “micromanaging.”<sup>12</sup>

Planning Organizational Missions and Functions. One important aspect of planning an organization’s mission and functions is to ensure their uniqueness. If an organization is perceived to be similar to another, even in another agency, it may be viewed as duplicative and, therefore, wasteful of taxpayers’ dollars. This is true at all levels of government. In times of constrained budgets, financial managers may act without full understanding of the circumstances or rationale underlying an organization’s existence. The leader should ensure that his organization’s mission is well justified, well publicized (at least to those who have a need to know, if classified), and well differentiated from others’ missions. While private sector organizations are not dependent upon taxpayer dollars, the same principle holds true. A dollar of cost is not a dollar of profit. Overlap in missions and

functions can lead to managerial challenges related to collaboration, sharing, de-confliction of operations, and other activities.

Planning Operations. The leader or manager of an organization must also plan the operations of the organization as well as its overarching mission and functions. Planning operations requires considering many factors: objectives, capabilities, resources, constraints, legal issues, and more. Perhaps the two most challenging aspects are (a) determining options to achieve one’s objectives most effectively and/or efficiently, and (b) developing implementation plans to guide all the disparate players who are involved in the operation.

In most intelligence organizations the principal operation is analysis. Planning for analysis involves many unknowns. Analysis is an intellectual endeavor that often defies deadlines and leads in unanticipated directions. As analysis is an intellectual process, imagination and innovation are important qualities for a manager to foster.

Resource Planning. Resources involve physical assets, money, and people. Physical assets already exist. Money can purchase future assets or capabilities. People can perform future tasks. As a manager is expected to accomplish his goals or objectives through coordinating the efforts of others, one of the principal responsibilities of a manager is to obtain the necessary resources. In all venues this requires careful planning. “One of the prerequisites for effective intelligence analysis anywhere and for any purpose is the availability of necessary resources—appropriately trained personnel, funds, and equipment.”<sup>13</sup>

A manager must know what resources exist and what is required to accomplish his mission. If a resource deficit exists this must be made known. Otherwise, the manager’s performance will suffer, as will his personnel performance evaluation. Every organization has a budget planning process. Understanding the managerial process of allocating funds (or reallocating them during the budget period) is essential, as illustrated in the following actual practical example.

#### *A Practical Example*

*On a Saturday morning in January 2002 at RAF Molesworth, United Kingdom, the Commander of the U.S. European Command’s Joint Analysis Center (JAC), a Navy captain, was working through a backlog of emails when he ran across an oblique reference to discussions of changes to the Department of Defense Unified Command Plan.\* While aware of the proposed UCP changes and the implication that they would give important new operational responsibilities to USEUCOM, in the hectic months since taking command*

---

*a few weeks prior to the attacks of 9/11 he had not focused on the implications of the UCP change on intelligence responsibilities.*

*What followed that early January “wakeup call” was an immediate action plan and months of energetic work to get approval for the resources that would be needed to implement the work required by the new responsibilities.*

*The JAC Commander’s key concern was not the scope or size of the intelligence tasks. Intimately familiar from previous tours and experience with the substance of the work, his concern was that he was late to the “budget game” of getting approval for the resources—people, dollars, equipment—needed to accomplish the new mission. While continuing support to existing missions, he had to develop and brief the resource needs for the new mission and implement a plan to begin all the new tasks well before 1 October. There was a very short window—only a couple of months—and a long list of key decision makers to convince in order to have any chance of getting new resources and to ensure readiness for the new tasks.*

*In mid-September came the official notification. Nearly all of the requested resources and new billets had been approved! After a few minutes to congratulate the team for its important victory in the resources battle, he reminded everyone that they would not actually see any of these new resources for at least six months.*

*The next day, the JAC Commander would return his focus to the preparations for support to a different Combatant Commander, U.S. Central Command (USCENTCOM), and what would be the invasion of Iraq. Where would the resources come from for those new combat support tasks? When would he pull people from existing tasks and what level of risk would he have to convey to his boss at EUCOM, his peers and other superiors in CONUS and, most importantly, the supported operational commanders, who were counting on his command for intelligence support?*

*\* DOD News Release No: 188-02, April 17, 2002: Unified Command Plan*

Besides planning for resources, a manager must be prepared to defend the resources already allocated to his activities at any moment. Financial managers (e.g., comptrollers) are always seeking unused, and therefore available, funds to apply to higher priorities in the organization. This often occurs quickly. If the operational manager is unprepared to defend his resources, his ability to affect the decision is forfeited.

Often before funds will be approved for an activity or operation, senior managers want to understand precisely how the funds will be spent. This requires the development of an implementation plan and an accompanying spending plan.

Knowing what resources already exist that could apply to one’s mission extends beyond the boundaries of a manager’s parent agency. This is true in government and the private sector. For example, there are reconnaissance capabilities funded in both the National Intelligence Program and the Military Intelligence Program.<sup>14</sup> Senior financial managers in the Executive Branch (especially in the Office of Management and Budget (OMB) in the White House) and Congressional committees will question requests for resources that appear to duplicate a capability that exists in another program or agency. Resource planners conduct “crosswalks” across programs to identify and eliminate (or justify) apparent duplication of efforts. A manager who advocates for a duplicative capability is often disappointed when final budget decisions are made. Therefore, a manager should seek how he can leverage the existing capability to his own mission’s benefit.

Planning for Human Capital. Planning for human capital is fundamental for management, especially in fields like intelligence that depend upon a skilled and trained workforce. Managers must plan for recruitment of new talent, for the retention of existing, trained personnel, and for succession of expertise in critical jobs to account for personnel loss or turnover. Education and training often are highlighted as necessary investments for intelligence personnel. The opportunity for advanced training is an important incentive for retaining talent in an organization.

A leader’s principal organizing responsibility is the selection and training of subordinate leaders. One problem highlighted by a former chief personnel officer is the tendency to equate technical competence (that is, subject matter expertise, or SME) with leadership potential. This is hardly a recipe for success. Leading and management skills, as well as knowledge of the intelligence discipline, are key qualities to identify in any potential candidate for filling key organizational positions.

Acquisition Planning. Understanding and managing the acquisition process is critical to ensuring future success of an organization. The Intelligence Community today, and even more so in the future, is highly dependent upon contractor support for everything from highly technical sensors and applications to analysts and maintainers of the IC’s complex information technology environment. Progress and key breakthroughs in difficult or rapidly developing intelligence problems are always best obtained when the intelligence operations, systems, and acquisition personnel



are working closely together with industry. Leadership is critical for acquisition. Leaders and managers at all levels need to plan carefully to bring to bear the right skilled personnel and the resources necessary for the envisioned program. Discipline needs to be imposed and enforced on the system requirements process. Moreover, strict controls need to be designed and implemented to ensure that managers know quickly of technical or resource problems that will affect success.

## 2. Organizing

This involves establishing the structure of the organization and who does what, including the boundaries of responsibilities and procedures.

There are many organizational models. Depending on mission, the leader of an organization will choose one or another model. The fundamental choice is between a centralized or decentralized model. A centralized model tends to push decision-making up the chain of command. The opposite is true for a decentralized model.

One model is the unitary organization. That is the traditional hierarchical structure best illustrated by a corporation with a CEO to whom senior vice presidents report. Vice presidents report to senior vice presidents. Directors report to vice presidents, and so forth. The structure is formal with defined lines of responsibility. The hierarchy of managers is often described as a "ladder." Historically, the military services had such a structure. Automotive manufacturing companies are another example.

The second model is the matrix organization, which is a more horizontal structure, and is characteristic of many large engineering firms. In such firms the vice president for engineering may be in charge of all engineers, but assigns them to work on various programs according to the needs of the individual programs. Matrix organizations have become more prevalent with the Information Age.

The third is a hybrid approach, which may exhibit characteristics of both a hierarchical organization and a matrix organization, or neither.

Within the National Intelligence Community can be found examples of all types of organizational structures. With the increasing complexity of intelligence collection, highly technical organizations were created to manage various intelligence disciplines (INTs). These specialty organizations were centralized and became known as "stovepipes." They managed the process of their specialties from cradle to grave. The National Security Agency (NSA) for signals intelligence (SIGINT) is a prime example. However, other organizations also became involved in

SIGINT, especially the military, the CIA, and the National Reconnaissance Office (NRO), leading to duplication of efforts.

What evolved out of this duplication was a new management model (a hybrid approach) referred to as "functional management." It began in the Department of Defense when the Defense Intelligence Agency (DIA) was assigned the budget planning authority for general military intelligence in the mid-1970s. The DIA Director was named as the functional manager for the General Defense Intelligence Program (GDIP), which incorporated the non-SIGINT programs of DIA and the four services. Later the NSA Director became the functional manager for SIGINT, with oversight and influence over the allocation of funds and program priorities for SIGINT efforts in the services, the NRO, and the CIA (to some degree). Within the Intelligence Community there are now numerous functional managers for different disciplines. Note that the functional management approach does not give the functional manager total management control. Much depends on cooperation. Functional management is a compromise between organizational management prerogatives and technical management of similar functions. Another partial compromise between centralized management and decentralized operation of intelligence activities is the mission manager concept instituted by the DNI. The mission manager is the "go to" official for a specific subject. The director of the National Counterterrorism Center (NCTC) is an example, coordinating counterterrorism activities across government as well as managing the Center itself.

Some organizations can have a very fluid management model. Google is one with a model described as an "adhocracy." As an entrepreneurial organization, with rapid growth, it would be impossible for Google to have a management structure like a government organization (nor could the government emulate Google). One fundamental point to keep in mind is that, being a private entity, a corporation measures its success or failure by its profit and losses. P&L is a wonderful, universal metric for companies. Government organizations obviously do not have the same. Of course, because the Intelligence Community is a government entity, its organization, mission, and functions, as well as many policies and procedures, are determined by politics.

Another successful organizational model developed and highlighted by GEN (USA, Ret) Stanley McChrystal in his book *Team of Teams* is worthy of consideration for intelligence missions. McChrystal served for five years, from 2003 to 2008, as Commander of the Joint Special Operations Command (JSOC). In *Team of Teams* McChrystal analyzes the history of modern management



and organization in the context of his own efforts to respond to the threat from the new and highly dynamic Al Qaida in Iraq, which resulted in dramatic changes in JSOC operations and in how his command leveraged, utilized, and integrated with the Intelligence Community. McChrystal realized that the availability and reach of 21<sup>st</sup> century information technology and the Al Qaida organizational model were enabling the enemy to move faster and have greater strategic impact than his highly trained and equipped special forces. His solution focused on exceptional levels of cross-organizational sharing and integration while also pushing responsibility far down the chain of command.<sup>15</sup> Deciding whether a centralized, decentralized, or a more radical “team of teams” model is best for the mission is a fundamental choice a leader and manager must make.

### 3. Directing

This involves guiding (and in some cases steering) the organization’s collaborative activities through communication and the development of policies and guidelines.

Clear written and oral communication is critical to effective direction. This is the function essential to the implementation of both plans and organizational guidelines. As Professor Manthorpe states:

[T]o successfully introduce and lead change, the leader must describe the intended results of the change in *specific* terms and set goals that are *clearly* achievable (emphasis added).<sup>16</sup>

The leader will set and affect the culture of the organization through the direction of activities over time. The policies for the organization should be explicit as to what is expected of the workforce in terms of ethics, behavior, priorities, and approaches to accomplish the mission. This includes setting and communicating the standards for teamwork, safety, and security, among other topics. A common military practice when assuming command is to publish a Commander’s Philosophy or Command Guidance. Typically only a single page, the Commander’s Philosophy sets the tone and lets everyone know what the new leader believes is important. For a Commander’s published philosophy to be of any value, of course, the leader’s actions and activities have to reflect the published words.

### 4. Controlling

Controlling an organization is like steering a sailboat. When wind conditions change, the skipper has to adjust the rudder to stay on course. To do this, of course, the skipper has to sense what has changed. This requires that the manager in

an organization maintain oversight of his domain and develop feedback mechanisms that allow him to know when to adjust the rudder. Communication channels must function both ways—down the organization from the manager and feedback up the organization to the manager. This requires that a manager be open to listening to subordinates and especially to bad news.

An interesting aspect of feedback is its motivational factor. Subordinates often yearn for recognition that they are doing their jobs well. For a manager (and especially a leader), providing positive feedback is important. Positive feedback is important even if the subordinate has made a mistake. He or she will already know that. What they need to know is how to do better in the future. Feedback focused on lessons learned is useful for the subordinate. It is also motivating.

We are a nation of laws, and they apply to the intelligence field as they do to every other endeavor. For managers of intelligence activities at every level, understanding the boundaries established by laws and regulations is an important component of controlling the organization. A challenge for the manager or overseer of business intelligence activities is the myriad laws and regulations at all levels of government and across jurisdictions that may apply to corporate activities. What may be acceptable in Wilmington, Delaware, may not be in San Jose, California. What may be acceptable in the U.S. may not be in the Republic of Korea or in China. Failure to adhere to the law is a management failure to properly control the activities of an organization and is rarely excusable.

Oversight is a managerial control mechanism. At the federal level it is an important check and balance mechanism among the branches of government. In government and business it is a fundamental tool for managers to understand progress, detect problems, and be able to re-plan, reorganize, and re-direct an organization’s activities, as necessary.

A leader or manager must know whether he is succeeding. How can he know if his vision is achievable or his plan is being met? Measuring effectiveness is not easy. Many activities do not lend themselves to easy quantification or measurement. A good example of setting a goal that could be measured came from President John F. Kennedy in his speech before a joint session of Congress on May 25, 1961:

I believe that this nation should commit itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to the earth.

Kennedy established three metrics—landing on the moon, returning safely, and within a specific time frame. The resulting Apollo program at the National Aeronautics and Space Administration was noted for its quantitative management metrics.

How does one measure the effectiveness of intelligence? A former executive director for the Intelligence Community, Rich Haver, wrote: “Intelligence is the simplest job in government. Our sole job is to know what our enemies don’t want us to know. Data are fine, information is better; if knowledge can’t be produced from the information we have failed. If the nation/leaders/decision makers are surprised we have failed.” Furthermore, “If intelligence knows what is going to happen but is unable to tell the story in a convincing enough manner that the decision makers do something about it, we have failed.”<sup>17</sup>

Haver’s standards are fine, but how does one measure them? Are they quantifiable? This is the fundamental problem in measuring intelligence. Its benefits often are observable only indirectly. In counterterrorism the detention or elimination of a known terrorist or the foiling of a specific plot is not an easy metric. A successful terrorist attack is also an easy metric of failure. Certain intelligence coups are metrics of success. For instance, a penetration of one’s adversary by an agent, or infiltration of a gang by a confidential informant, is a metric of success, especially as the deep penetration of the enemy is the prime objective of any intelligence service.

As intelligence can be viewed as a process, metrics can and should be employed at every step of the process (i.e., the “intelligence cycle”) to understand where the resources and assets are being used. Output from sensors must be evaluated to determine what requirements are not being met. The number and levels of analysts assigned to various problem sets must be determined and continuously reassessed based on the prioritization of customer demands, available sensor collection and the ability of the analysts. Short- and long-term storage of data must be constantly measured and the need for additional or newer information technology must be identified, programmed for, and installed.

The most important set of metrics must be focused on the decision-makers. How, when, and where is the organization “touching” the customer? What feedback is being received? The constant question to be answered revolves around how the entire organization’s capacity for providing decision advantage can be expanded to meet the highest number and most important problems. In an article entitled “Determining Measures of Success,” Neil Simon, a business consultant writing for intelligence professionals, posits “the point to remember is that your sponsors and customers determine

your success: being successful as a unit means identifying their expectations and meeting their needs.”<sup>18</sup> The ultimate assessment of intelligence as to its value has to come from clients and consumers of intelligence.

Understanding “outcomes” through measures of effectiveness or performance is important for operational managers. Without these, there is no rational basis for applying resources to competing needs. There is always greater demand for intelligence than there is capability. Partly, this is due to the fact that the clients and consumers of intelligence do not have to pay for it directly. The costs are indirect and largely invisible to those who demand to receive intelligence support. The manager of intelligence, therefore, has to allocate his resources (or capability) judiciously and with agility. Rationing scarce resources requires understanding where one can get the “most bang for the buck.” Generally, in the intelligence business, people are the most important resource and tracking closely what, where, and how people are affecting intelligence capacity is critical. Metrics are also important in answering the question, “When is enough enough?”

The real impact of metrics is that they impose a discipline on managers that is important. Remember Warren Buffett’s observation: “Lacking...standards, managements are tempted to shoot the arrow of performance and then paint the bull’s-eye around wherever it lands.” Over time this is a recipe for failure.

## PROTECTING SOURCES AND METHODS VERSUS OPENNESS

For a leader and manager in intelligence, security is and must be a central issue. Failure to maintain security for sensitive activities can lead to their failure, and worse. Sharing of information requires a measure of openness. Security, on the other hand, requires protecting the identity of sources and the methods used for information gathering and analysis. There is a fundamental friction between security and sharing. The classifying of information and restricting its dissemination are two age-old approaches to ensuring secrecy.

One of the long-standing cultural issues that have impeded intelligence sharing is the ownership concept. Agencies that collected intelligence data exercised close supervision over its dissemination, sharing, and use. CIA controlled human source intelligence through a caveat of “Originator Controlled,” or ORCON, which meant that CIA had to give permission for the intelligence to be disseminated further or shared with persons not previously approved to receive the intelligence. NSA also employed similar techniques for

communications intelligence. The FBI also has been reluctant to share with other law enforcement entities intelligence it gathered. How much this reluctance is due to security concerns or ownership issues is open to debate.

The WikiLeaks revelations by Private Bradley Manning and the exposure of signals intelligence and other secrets by Edward Snowden are the consequences of not understanding and not managing closely enough the risks from advanced information technology. Both cases reflect leadership and managerial failures. Manning downloaded a half-million military messages and 250,000 diplomatic cables from 271 U.S. embassies and consulates in 180 countries when assigned to Forward Operating Base Hammer, near Baghdad, in 2010. He leaked these to WikiLeaks. The lack of adequate controls, oversight, and awareness of the significant damage potential from an insider threat allowed a disturbed person access to classified information far beyond his need to know (the long-standing basic principle for access to classified information). Manning had been identified as unstable and a risk to deploy to Iraq but, given a shortage of intelligence specialists, management in the 10<sup>th</sup> Mountain Division ordered him to deploy nonetheless.<sup>19</sup> One management failure relates to the decision maker being ignorant of the personnel and potential security issue. The equally, if not more important, issue is the continued lack of leadership focus on the risk and the absence of adequate security controls.

The Snowden affair reveals multiple managerial failures regarding security. His background investigation was faulty, conducted by a contractor which cut corners to increase revenue and for whom oversight was deficient. An adverse CIA personnel report (for trying to access unauthorized information) was not shared with NSA security clearance adjudicators who provided Snowden high-level access to compartmented information. Snowden's practice of "borrowing" passwords was either undetected or ignored by his managers in Japan and Hawaii. Moreover, his undeclared and unauthorized travel to India in 2010 failed to register with counterintelligence personnel.<sup>20</sup> In each instance these were failures to adhere to existing policy and were unnoticed or dismissed by relevant managers within various agencies. The consequences of both Manning's and Snowden's leaks have been devastating to U.S. intelligence, U.S. diplomatic relations, and U.S. allies.

Both the Manning and Snowden cases, as well as the persistent penetration of U.S. government and contractor networks by adversary nation-states, all share as a root cause a breakdown by people, not technology. The advanced capabilities of today's cyber hackers/spies have significantly increased the impact of these cases, but the problems—and the solutions—are most dependent upon organizational leadership and effective management which recognizes mission risk and the fact that human beings and technical systems all will have failures. Leaders and

subordinate managers must always assess risk versus gain in everyday decisions, and there must be a high level of engagement and thinking to mitigate the damage from failures related to information technology systems.

## CONCLUSION

The leader/manager of any organization must take a holistic view. Managing only a portion of an organization or activity is a recipe for failure. A core principle of intelligence mission management is leading all parts of an organization to maximize the timeliness, relevance, and decision impact of the intelligence it produces. The director or commander of an intelligence organization cannot lead *OR* manage—he/she has to do both, at the same time, all the time. Leadership and management are inseparable.

Our nation's future national security is highly dependent upon the capacity of our Intelligence Community to support decision-making at every level, from the White House to the foxhole. Our sensors, systems, organizations, and processes must be continuously evaluated and improved at the most efficient cost. Our intelligence personnel and contractors must all be simultaneously supported and challenged to produce more quantity while maintaining the quality of intelligence. There has never been a more important task ahead of us than in improving leadership and management of intelligence.

## NOTES

<sup>1</sup> Much of this discussion benefits from Professor William H.J. Manthorpe's former course on leadership for intelligence professionals, titled Learn to Lead, taught at the then-National Defense Intelligence College.

<sup>2</sup> Business school professor J. Thomas Wren of the University of Richmond's Jepson School of Leadership Studies, editor of *The Leader's Companion: Insights on Leadership through the Ages* (New York: The Free Press, 1995).

<sup>3</sup> James McGregor Burns, an authority on leadership studies and Woodrow Wilson Professor Emeritus of Political Science at Williams College, in J. Thomas Wren, *The Leader's Companion*.

<sup>4</sup> Wren, in *Ibid*.

<sup>5</sup> John P. Kotter, Professor of Organizational Behavior at Harvard Business School, and one of the leading proponents of making the distinction between management and leadership, in *A Force for Change: How Leadership Differs from Management* (New York: The Free Press, 1990).

<sup>6</sup> Joseph S. Nye, *The Powers to Lead* (Cambridge, MA: Harvard University Press, 2008). Professor Nye is well qualified to discuss leadership in government, having served as Under Secretary of State, Assistant Secretary of Defense, and Chairman of the National Intelligence Council.

<sup>7</sup> Aristotle as quoted by Joseph S. Nye in the preface of *The Powers to Lead* and by Aristotle in *Politics*.

<sup>8</sup> Manthorpe, *Learn to Lead*.

<sup>9</sup> William O. Studeman, email to co-author Peter C. Oleson, August 4, 2010.

<sup>10</sup> Richard L. Shell, *Management of Professionals*, revised edition (New York: Marcel Decker, Inc., 2004).

<sup>11</sup> Ronald Heifitz and Lawrence Lindsey in "Leadership on the Line," address to the Navy's Executive Business Course at the Naval Postgraduate School. Heifitz is the founding director of the Center for Public Leadership at the John F. Kennedy School of Government at Harvard University. Lindsey was director of the National Economic Council in the White House, 2001-2002, and previously was on the board of governors of the Federal Reserve System, 1991-1997.

<sup>12</sup> General Jones made these comments to President Obama when interviewed to be his National Security Advisor. Bob Woodward, *Obama's Wars* (New York: Simon and Schuster, 2010).

<sup>13</sup> Don McDowell, *Strategic Intelligence: A Handbook for Practitioners, Managers and Users*, revised edition (Lanham, MD: The Scarecrow Press, 2009), pp 59-60.

<sup>14</sup> The National Intelligence Program (NIP) is managed by the Director of National Intelligence and funds intelligence activities that support multiple departments and agencies of the government. The Military Intelligence Program (MIP) is part of the Department of Defense budget and funds activities supporting the Department and the military services.

<sup>15</sup> Stanley McChrystal, *Team of Teams* (New York: Penguin Publishing, 2015).

<sup>16</sup> Manthorpe, *Learn to Lead*.

<sup>17</sup> Rich Haver, email to Peter C. Oleson, August 2, 2010.

<sup>18</sup> Neil Simon, *Competitive Intelligence Magazine*, Vol. 1, No. 2, July-September 1998, p. 47.

<sup>19</sup> John Sellers, "Why insider threats keep succeeding," *FCW*, May 8, 2015 <http://fcw.com/Articles/2015/05/08/comment-why-insider-threats-keep-succeeding>.

<sup>20</sup> Peter C. Oleson, "Assessing Edward Snowden: Whistleblower, Traitor, or Spy?" *The Intelligence*, *Journal of U.S. Intelligence Studies*, Vol. 21, No. 2, Summer 2015, Association of Former Intelligence Officers.

*Peter Oleson is a former assistant director of the Defense Intelligence Agency, senior intelligence policy advisor to two Secretaries of Defense, chief executive officer of a technology consulting firm, and associate professor of management in the graduate school of the University of Maryland University College. He is a member of the board of the Association of Former Intelligence Officers and editor of its recently published Guide to the Study of Intelligence.*

*RADM (USN, Ret) Tony Cothron was a career Naval intelligence officer and the 63<sup>rd</sup> Director of Naval Intelligence. He commanded the Office of Naval Intelligence and the USEUCOM Joint Analysis Center and led operational intelligence efforts during combat in DESERT STORM and Kosovo.*



# INTELLIGENCE

## Empowering Decision Makers

When national security is at stake, CACI provides the intelligence tools and tradecraft to deliver critical information. Our intelligence team leverages all sources of information to empower decision makers. From commanders in the field to policy-makers across government, we provide our customers with the knowledge they need to succeed against foreign and domestic threats.

Learn more at:  
[www.caci.com/Intelligence\\_Services](http://www.caci.com/Intelligence_Services)

A Fortune World's Most Admired Company

**CACI**  
EVER VIGILANT

©2016 CACI - 0166, 1612





---

# Activity-Based Intelligence: Coping with the "Unknown Unknowns" in Complex and Chaotic Environments

by Col (USAF) James L. Lawrence II

---

We're swimming in sensors and we need to be careful we don't drown in the data...the unavoidable truths are that data velocities are accelerating and the current way we handle data is really overwhelmed by this tsunami...so we're going to have to begin exploring different ways to meet the growing challenges of hyper-scale workloads.

—Lieutenant General (USAF, Ret) David Deptula<sup>1</sup>

## INTRODUCTION

Over the past decade, military and civilian leaders throughout all levels of the U.S. government have voiced their insatiable demand for more intelligence information in order to successfully prosecute a war against al Qaeda and its affiliate groups, as well as to thwart other violent extremist organizations around the globe. It is not by chance, then, that the call from decision-makers for more intelligence at all levels coincides with the steady upsurge of sensors, systems, and platforms augmenting the nation's intelligence-gathering arsenal. The rationale behind the acquisition of more intelligence systems is incontestable and straightforward: intelligence plays a vital role in the decision-making process. Military commanders in Afghanistan, for example, continue to rely heavily on intelligence information in order to execute both counterterrorism and counterinsurgency actions. Likewise, the importance of intelligence information to national decision-makers becomes apparent when viewed through both strategic and financial lenses.

From a strategic perspective, the significance of intelligence is highlighted several times throughout the May 2010 National Security Strategy, stressing that "our country's safety and prosperity depend on the quality of the intelligence we collect and the analysis we produce, our ability to evaluate and share this information in a timely manner, and our ability to counter intelligence threats."<sup>2</sup> From a budgetary standpoint, the value of intelligence throughout the Department of Defense (DOD) has steadily increased since 2002. In fact, FY 2010 saw DOD commit in excess of \$80 billion toward the nation's ISR enterprise—

comprised of entities within both the national and military intelligence communities—in order to develop and acquire new ISR capabilities.<sup>3</sup>

---

*This article argues that the IC should consider adopting an activity-based intelligence methodology in order to better address complex and chaotic problem sets to more effectively synthesize data into finalized intelligence for use by commanders and decision-makers.*

---

Yet, a concern is emerging among analysts within the IC that the steady growth of the ISR enterprise is complicating the processes and methodologies utilized to produce finalized intelligence. Specifically, the nature of operations in Afghanistan, coupled with the rapid growth of ISR sensors, systems, and platforms have revealed the inefficiencies associated with object-based intelligence production (i.e., cause and effect analyses that focus on a single source or object). Ultimately, this flood of information has overwhelmed the Intelligence Community (IC) with more data than it can effectively process, exploit, and disseminate to end users as finished intelligence. Thus, the purpose of this paper is threefold: (1) to highlight the issues surrounding object-based intelligence collection and analysis in counterinsurgency operations using Afghanistan as an example; (2) to discuss how the nature of intelligence support during counterinsurgency and counterterrorism operations in Afghanistan revealed inefficiencies of community-standard analytical processes; and (3) to describe the activity based intelligence methodology, and argue how this analytical process might best serve the IC in developing finalized intelligence for use by decision makers at all levels. This article argues that the IC should consider adopting an activity-based intelligence methodology in order to better address complex and chaotic problem sets to more effectively synthesize data into finalized intelligence for use by commanders and decision-makers.



---

## EXPANDING THE ISR ENTERPRISE

### More (and Better) ISR Hardware, Same Analytical Framework

**I**ncreasing DOD's ISR arsenal to meet the demands of a growing customer base to combat violent extremism around the world is relatively justifiable. In some regard, however, the amount of money dedicated toward expanding the ISR enterprise with increased sensors, systems, and platforms (i.e., hardware) only exacerbates a longer-term issue: how does the IC adapt its analytical framework (i.e., processes and methodologies) to operate within denied and contested environments in future conflicts? DOD's ISR acquisition strategy leaves room for concern. To illustrate, a 2012 audit of the acquisition program found that since 9/11 roughly \$44 billion have been allocated toward purchasing new and enhanced ISR capabilities—with the emphasis placed on Unmanned Aerial Systems (UAS).<sup>4</sup> Furthermore, the majority of DOD spending toward ISR has been devoted to the UAS fleet, multiplying an inventory total of just 167 aircraft back in 2002 to more than 7,500 aircraft in operation today.<sup>5</sup> Curiously, the audit makes no mention of any funding dedicated toward, or the need to invest more in, developing and improving the analytical framework required to produce finished intelligence.

Consequently, the lack of oversight of the ISR acquisition process by DOD has resulted in countless ISR assets now in operation—overtaking the IC's ability to adapt and develop its own analytical processes in order to keep pace within the current operating environment. Senior leaders must realize that a balanced ISR strategy “should provide clear, focused direction, and create a shared context that orients the ISR enterprise toward problem solving over production.”<sup>6</sup> Therefore, caution is warranted for those who assume that ISR enterprise expansion also takes into account the robust analytical framework required to produce finished intelligence. Both are essential to ensure leaders at all levels have the information required for ISR analysis, strategy development, and decision-making.

Additionally, a majority of ISR platforms were scheduled to return to the United States at the end of 2014, as our commitments in Afghanistan began to decrease. This massive redeployment of resources left DOD with the decision of how to smartly reallocate these assets to combatant commanders in anticipation of the next major conflict.<sup>7</sup> Though the operating domains for ISR in Afghanistan were mostly uncontested, the complexity associated with analyzing and producing finished intelligence proved challenging. Hence, the prospect of the IC's ability to produce finished intelligence utilizing its current analytical framework while operating in a contested and denied environment seems daunting. For further clarity,

the following vignette gives perspective on intelligence operations conducted in Afghanistan throughout the counterinsurgency campaign. Specifically, the example highlights the dilemma of utilizing a cause-and-effect type of analytical framework in a complex, albeit uncontested, operating environment. The example also infers that the IC should consider an analytical paradigm shift in order to operate successfully in the contested and denied environments of the future.

### COUNTERINSURGENCY: INTELLIGENCE OPERATIONS IN A COMPLEX ENVIRONMENT

#### Contrasting Viewpoints of Intelligence in Iraq and Afghanistan

**T**he nexus between relevant intelligence information and decision-making has been crucial throughout the ongoing counterinsurgency fight in Afghanistan. While this information has been developed utilizing a variety of sources and methods, the disciplines of signals intelligence (SIGINT), geospatial intelligence (GEOINT), and human intelligence (HUMINT) have been the most prolific. However, unlike the success of intelligence portrayed by III Corps leadership in Iraq during Operation IRAQI FREEDOM,<sup>8</sup> previous International Security Assistance Force (ISAF) leadership in Afghanistan has offered a more pragmatic characterization. Similar to III Corps in Iraq, ISAF suggested that intelligence in counterinsurgency operations begins at the lowest echelon—shaping the decision-making process of commanders and leadership at the operational and strategic levels of warfare.<sup>9</sup> Additionally, leaders in Afghanistan realized the value of small groups of analysts working together in Intelligence Fusion Centers; the synergy between military and civilian analysts significantly increased the throughput of direct intelligence support to kinetic operations. As a result, intelligence leaders in Afghanistan lauded the fact that “Fusion Centers were able to coordinate classified SIGINT and HUMINT, and real-time surveillance video, allowing commanders to ‘action’ the information with airstrikes and special operations that led to the death or capture of notorious terrorists...”<sup>10</sup>

Nevertheless, the perceived issues with intelligence in Afghanistan did not center on any particular discipline or its application primarily; i.e., there were no issues raised regarding how well or how poorly the IC conducted SIGINT, HUMINT, or GEOINT. Rather, ISAF personnel argued that the degree of emphasis placed on collection efforts and analytical processes directed toward finding, capturing, and/or killing insurgents negated the IC's ability to answer fundamental questions about the overall operational environment,<sup>11</sup> thereby limiting ISAF's overall

counterinsurgency efforts to protect and gain the trust of the local populace. Furthermore, the catalyst behind the IC's focus on insurgents was attributed to the extremists' tactic of using improvised explosive devices (IEDs) against coalition forces. According to ISAF, coalition efforts to spot insurgents emplacing IEDs using aerial drones "baited intelligence shops into reacting to enemy tactics at the expense of finding ways to strike at the very heart of the insurgency."<sup>12</sup> Moreover, ISAF characterized intelligence efforts to discover insurgent networks as "labor-intensive," leading to reactive methods which provided little new information to the brigades and regional commands. Moreover, lethal targeting of insurgents (i.e., counterterrorism targeting) would not help U.S. and allied forces ultimately win the war in Afghanistan.<sup>13</sup> In essence, the object-based intelligence focus on insurgents and IEDs in Afghanistan—coupled with the analytical framework used to defeat them—underscored the community's need to reconsider its approach to intelligence analysis.

The complex nature of counterinsurgency operations in Iraq and Afghanistan demanded the continual passing of information to leaders at all levels. Likewise, both ISAF and III Corps leadership acknowledged and successfully demonstrated that critical intelligence often materialized from the lowest organizational echelon—with small cells of focused analysts dedicated to developing intelligence, driving operations, and informing commanders and strategic-level decision-makers. Still, how can the characterization of the quality of intelligence production vary so greatly given the similar counterinsurgency tenets and tactics experienced in both Iraq and Afghanistan? I would submit that much of the disparity regarding the success of intelligence operations in each conflict is not the result of one intelligence discipline versus the other, nor the level from where the intelligence was produced. Rather, many of the discrepancies encountered resulted from the linear analytical processes and methodologies used to produce finalized intelligence in a complex and dynamic counterinsurgency environment.

## THE PROBLEM WITH INTELLIGENCE ANALYSIS TODAY

### The Reactive Nature of Current Intelligence

Intelligence analysis is a cognitive activity—both art and science—applying tools and methods to collected data and information in order to create and deliver intelligence knowledge, with the goal of providing decision advantage to commanders and decision makers.<sup>14</sup> Given this definition, an accurate depiction of intelligence analysis in Iraq and Afghanistan is best categorized as both tactically focused and operationally relevant. In general, both the intelligence resources and activities today (whether derived from a

forward-deployed field unit or within a national intelligence agency) focus primarily on tactical intelligence reporting as opposed to longer-term analysis of adversary intentions.<sup>15</sup> Several reasons account for the over-saturation of this type of intelligence reporting; however, a major contributing factor is the ubiquitous nature of sensors, systems, and platforms capable of providing nearly instantaneous SIGINT and GEOINT data to the lowest-echelon warfighter.<sup>16</sup> Before these current conflicts, intelligence data could take days or weeks to process, with the bulk of collection primarily reserved for intelligence analysis focusing on solving longer-term issues.<sup>17</sup> At present, and in specialized cases, an enormous amount of intelligence data has been made available directly to those personnel in direct support of ongoing operations, which continues to be the norm today.<sup>18</sup>

Another contributing factor to the reactive nature of intelligence operations may be the result of a common analytical practice currently utilized by several organizations within the IC. This practice is based largely on categorization modeling, whereby a simple framework is developed (e.g., a pattern-based scale derived from the unique characteristics or performance measurements of, for example, a person or an object), data are collected from a person or an object and input into the framework, and then the person or object is categorized based on its output characteristics.<sup>19</sup> Thus, in categorization modeling the pre-established framework precedes the available data, ultimately allowing for faster analysis that is good for intelligence exploitation. However, is not ideal for in-depth exploration or during periods of change.<sup>20</sup>

The reliance on categorization modeling by some within the IC might explain the reactive nature of intelligence operations—particularly when applied to rapidly adaptive problem sets such as insurgent locations and IED networks in Afghanistan. Similarly, the current emphasis placed on immediate reporting by senior-level decision-makers and military commanders alike is more prevalent now, as is the ability to provide nearly instantaneous military intelligence essential to end-users conducting day-to-day operations.<sup>21</sup> However, it is necessary that the IC consider other frameworks that focus not only on immediate, exploitive analysis, but methodologies that provide more fidelity to longer-term problems requiring analytically-based solutions.

## MODELING FOR LONG-TERM INTELLIGENCE ANALYSIS

### The Cynefin Framework

Further explanation regarding why the IC relies so heavily on categorization modeling involves a fundamental assumption found in organizational theory and practice: that a certain level of predictability and

order exists in the world.<sup>22</sup> Moreover, this assumption encourages simplifications that are useful in ordered circumstances. However, as circumstances change the simplifications have the tendency to fail.<sup>23</sup> An alternative method to categorization modeling is the Cynefin (pronounced ku-nev-in) Framework, which affords intelligence analysts and decision-makers the opportunity to see things from alternate viewpoints, assimilate complex concepts, and address real-world problems.<sup>24</sup> Specifically, the Cynefin Framework is a decision-making or analytical framework that recognizes the causal differences existing between system types and proposes new approaches to decision-making in complex social environments.<sup>25</sup> Unlike categorization modeling, where the framework itself precedes the data input, the Cynefin Framework is a sense-making model in which the framework emerges from the data itself.<sup>26</sup>

The Cynefin Framework consists of five domains: (1) the simple domain, where cause-and-effect relationships exist, are predictable, and are repeatable; (2) the complicated domain, where cause-and-effect relationships exist, but are not self-evident and therefore require expertise to decipher; (3) the complex domain, where cause and effect are only obvious in hindsight, with unpredictable and emergent outcomes; (4) the chaotic domain, where no cause-and-effect relationships can be determined; and (5) disorder, where decision-makers or analysts do not know the domain in which they reside.<sup>27</sup> Similar to characterization modeling, the simple and complicated domains of the Cynefin Framework are where most intelligence analysis occurs in order to determine causal relationships. However, the events of September 11, 2001 (chaotic), and the subsequent conflicts in Iraq and Afghanistan (complex) are the domains within which the IC has operated for the past decade. To meet these challenges, the IC must seek more accurate mental models and better analytical tools in order to gather, synthesize, and determine the meaning behind the ambiguous and conflicting information of the complex and chaotic domains. Therefore, processes such as categorization modeling utilized by intelligence analysts must adapt in order to deal with more complex and chaotic problem sets faced currently and in the future.

## ACTIVITY-BASED INTELLIGENCE

### Coping with the “Unknown Unknowns”

**T**he bulk of the IC’s analytical problems reside within the complex and chaotic domains of the Cynefin Framework. Moreover, the complex domain—the realm comprised of the “unknown unknowns”<sup>28</sup> and laden with unpredictable outcomes—warrants the most attention from analysts and decision-makers alike. Gregory Treverton offers a perspective regarding the “unknown unknowns” concept, likening the shift in the majority of intelligence

problem sets today from “puzzles to mysteries.”<sup>29</sup> Treverton compares puzzles to that of *known* problems, whereby new information will solve the puzzle.<sup>30</sup> Mysteries, however, are *knowable* problems, whereby an analyst may not necessarily know the answer to the problem, but might know what activities and events to look for in order to establish relationships.<sup>31</sup> [Editor’s Note: At the time the paper on which this article is based was written, Dr. Treverton was a longtime noted analyst at the RAND Corporation. He is currently Director of the National Intelligence Council (NIC) under the Office of the Director of National Intelligence.]

---

*Gregory Treverton offers a perspective regarding the “unknown unknowns” concept, likening the shift in the majority of intelligence problem sets today from “puzzles to mysteries.”*

---

An example of this concept involves the state of the Iranian nuclear program discussed in a 2007 National Intelligence Estimate (NIE). New information provided in the NIE revealed a solution to an IC puzzle—namely, where does Iran’s nuclear weapons program stand, or where did it stand circa 2003?<sup>32</sup> Furthermore, questions addressed in the NIE regarding the overall status of Iran’s nuclear enrichment capabilities disclosed answers to both puzzles and mysteries. For example, the technical aspects of the enrichment program itself provided answers to puzzles such as “how many centrifuges?” and “what level of production capacity?” while the critical questions such as “what happened to Iran’s enrichment program after 2003?” still remain mysteries.<sup>33</sup> Therefore, it is necessary that the type of intelligence discipline utilized within the complex domain be capable of dealing with the mysteries encountered in addressing the “unknown unknowns.” Activity-based intelligence (ABI) is an example of an emerging intelligence discipline that may satisfy this need.

ABI is characterized as a discipline of intelligence whereby the analysis and subsequent collection are focused on the activity and transactions associated with an entity, a population, or an area of interest.<sup>34</sup> Furthermore, the Human Domain, or Human Dimension—as an integral component of the ABI discipline—comprises several factors. These factors include presence, activities (including both physical and virtual transactions), culture, social structure/organization, networks and relationships, motivation, intent, vulnerabilities, and capabilities of humans (single or groups) across all domains of the operational environment (space, air, maritime, ground, and cyber).<sup>35</sup> ABI enables intelligence analysts to shift away from an object-based focus and more toward collecting data on activities and transactions over



long times or large areas. This allows for the storage and archiving of large amounts of ABI data into a database for future analysis. These large data sets can be “mined” for unknown unknowns, i.e., relationships or activities that were previously unrecognized.<sup>36</sup>

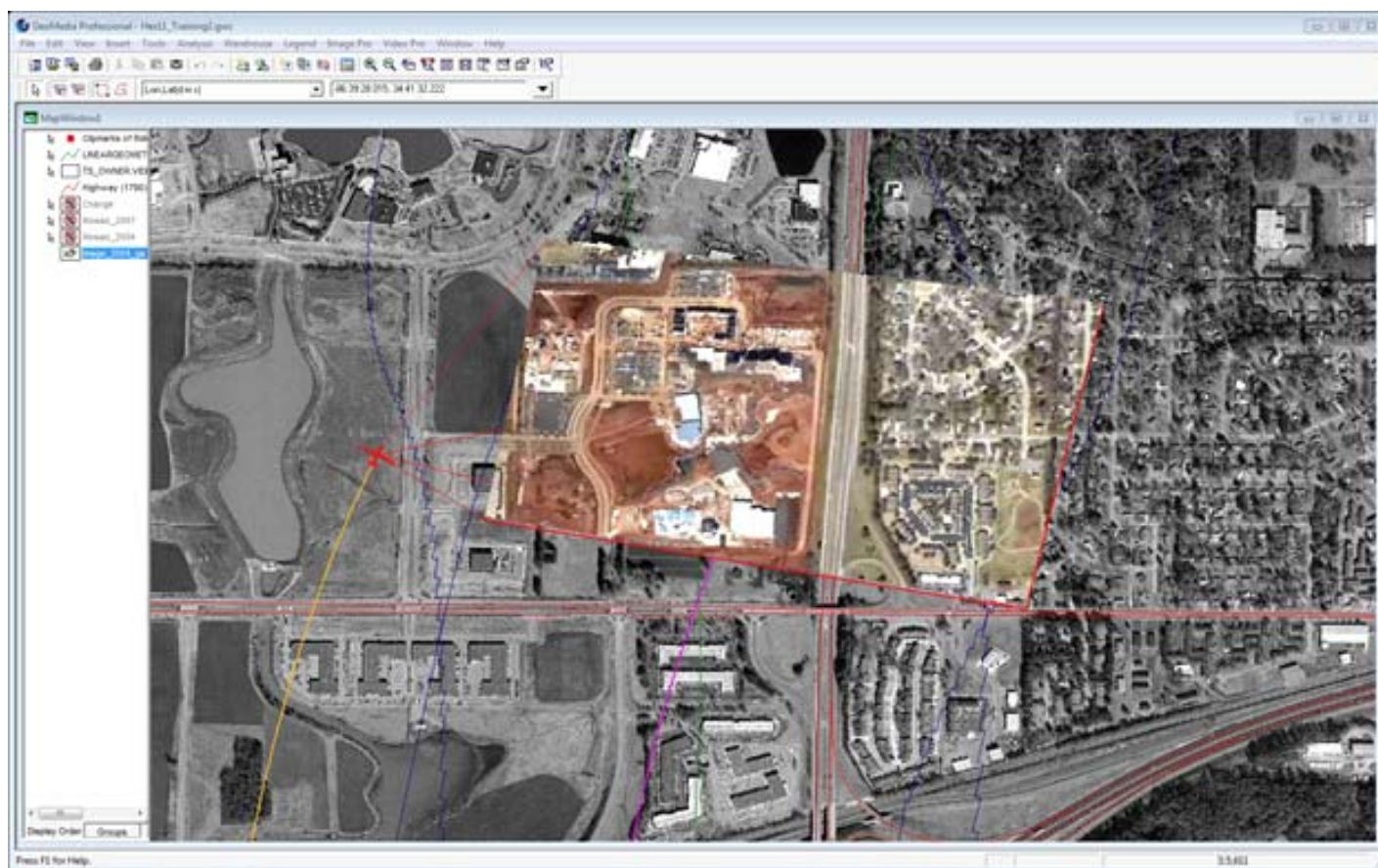
### Reemergence of ABI

Previously I described the contrasting views of counterinsurgency intelligence and analysis from the perspectives of III Corps personnel in Iraq and ISAF personnel in Afghanistan. Though each command organization offered differing views regarding intelligence effectiveness, both agreed that certain intelligence disciplines—namely, SIGINT, GEOINT, and HUMINT—were integral to commanders and decision-makers in providing near-real-time situational awareness throughout the counterinsurgency campaign. Likewise, special operators in Iraq and Afghanistan reached back to intelligence analysts at the National Geospatial-Intelligence Agency (NGA) to assist them with filling in tactical intelligence gaps.<sup>37</sup> In turn, the analysts began compiling information gathered from a range of intelligence disciplines—from SIGINT and HUMINT to open source reporting—geotagging the

information and storing the data into a database that (when queried) could be used to establish insurgent locations and networks.<sup>38</sup> For example, a common ABI format is referred to as activity layer plots. An intelligence analyst may superimpose all geotagged intelligence information about an IED explosion atop other intelligence information denoting a kidnapping in the same area. The analyst could then layer in other various open source data involving the same area and, once displayed, derive further intelligence information not seen or tracked before prior to the original IED event taking place.<sup>39</sup>

### Characteristics of ABI

ABI as an intelligence discipline is nothing new per se. In fact, the synthesis of complex pieces of information gained as a result of painstaking network or nodal analysis and human terrain mapping have been practiced for years within the IC. However, it is the advancement in technology, such as cloud computing, emerging new data sources, and developments in the processing of large data sets both rapidly and efficiently, which now makes ABI possible to execute on a large scale.<sup>40</sup>



A sample ABI product displaying real-time unmanned aircraft system video feeds and other geospatial data over a satellite image. Adapted from *Earth Imaging Journal*, <http://ejjournal.com/2013/is-activity-based-intelligence-a-modern-crystal-ball>.

The ABI methodology can be organized into four not necessarily sequential characteristics: (1) persistently collecting data on activity and transactions over a broad area or with a variety of sources, and then storing it in a searchable database; analysis of the data may happen immediately or that data may not become relevant to an intelligence issue until much later; (2) “sequence neutrality,” which looks for clues in the data, both backward and forward in time; (3) “data neutrality,” or the idea that all data are useful; analysis should not be biased toward any one data source, and (4) “knowledge management.” That is, when the ABI methodology is used to uncover associations in data it is important to capture them in a knowledge system using smart metadata tagging so they can be retrieved in the future.<sup>41</sup> While ABI methodology may be ideal to solve intelligence issues dealing with complex problem sets now and in the future, several issues must be addressed prior to the ABI methodology being accepted as a long-term IC solution.

---

*Adoption and implementation of the ABI methodology by the IC is a natural progression from analytical categorization modeling, given the unpredictable and emergent outcomes encountered in the complex domain faced in Iraq and Afghanistan.*

---

## CHALLENGES AND RECOMMENDATIONS

**A**doption and implementation of the ABI methodology by the IC is a natural progression from analytical categorization modeling, given the unpredictable and emergent outcomes encountered in the complex domain faced in Iraq and Afghanistan. However, there are three pressing issues that must be addressed prior to ABI methodology becoming the norm among IC analysts: (1) the need to invest in a solution to seamlessly archive and access vast amounts of ABI data stemming from various sources and systems; (2) the need to drastically improve information integration and enterprise-wide interoperability; and (3) the need to train and to educate analysts on the benefits of utilizing the ABI methodology to address complex and chaotic problem sets.

### ABI and the Data Storage Dilemma

Issues to overcome prior to Community-wide acceptance of an ABI methodology include finding a solution to the ABI data storage and retrieval dilemma. ABI is comprised of various intelligence disciplines encompassing multiple

phenomena, locations, timelines, and confidence levels, that is, “Big Data” so complex and so large that it presents a demanding technological challenge to overcome.<sup>42</sup> Also, “Big Data” is further complicated by the speed at which these data are now created—resulting in a solution that must account for exponential growth—and the disparate origins of information that may present challenges to analytical synthesis.<sup>43</sup> DOD recognizes these challenges; however, many previous solutions have attempted to centralize the data into repositories, or dictate specialized or complex data structures that were not necessarily applicable to all end-users.<sup>44</sup>

A potential solution to the challenges presented by ABI data storage and access is the continued development of, and investment in, cloud computing architecture. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.<sup>45</sup> Currently, the NGA’s NSG Expeditionary Architecture (NEA) holds promise as a Community-wide ABI data storage and retrieval system built on cloud architecture. The “NEA Cloud” holds both exploited and raw, unexploited data that—when combined—allow access to both activity-based association data and metadata. These data, along with other analysis from various sources, will provide analysts with an amalgam of information in which to develop patterns of life, discover networks, conduct nodal analysis, and determine abnormalities which may have otherwise been overlooked.<sup>46</sup> The way forward, then, is to continue development and expansion of the NEA Cloud and to ensure its unfettered access by national- and service-level intelligence analysts throughout the Community.

### Improving Data Integration and Interoperability

A similar challenge to that of ABI storage and retrieval is the interoperability of data-gathering systems. Many sensors, systems, and platforms which comprise the ISR enterprise were planned, developed, and operationally employed for specific purposes—not designed necessarily to be compatible with one another. Furthermore, each service possesses its own command and control structure for its portion of the ISR enterprise, resulting in a greater divide in achieving worldwide systematic interoperability.<sup>47</sup>

DOD also recognizes the issues with interoperability, and has efforts underway to improve systematic integration across the board utilizing a phased approach. The first phase includes connecting existing systems belonging to



the military services—so that each service has an interoperable “family” of systems. Phase two focuses on interconnecting the families of systems to ensure joint and combined forces have unprecedented common access to battlefield data.<sup>48</sup> While the framework to address interoperability issues across the board is in place, the incorporation of a relatively new ABI methodology has only just begun to be included as part of the discussion necessitating the urgency of interoperable systems. Yet, as ABI applications and tradecraft evolve as warfare evolves, technology and interoperability must be at the forefront of the solution to allow intelligence analysts to support operations anywhere in the world.<sup>49</sup>

### Building a Better Analyst

The final consideration prior to adoption of the ABI methodology by the Intelligence Community writ large is formalized training and education. Analysts within the IC generally subscribe to categorization modeling. While adequate for use within the simple and complicated domains, ABI methodology requires further training for analysts to better address intelligence problem sets residing in the complex and chaotic domains. This training should allow ABI analysts to look at a variety of data types and determine their reliability, outline basic patterns of inference, examine the obstacles that arise based on cognition and small-group processes, differentiate between “puzzles” and “mysteries,” as well as distinguish between tactical and long-term intelligence analysis.<sup>50</sup>

Lastly, any training program that teaches ABI methodology should emphasize the ultimate goal of assessing uncertainty:

In this view, it makes little sense to seek a single “right answer” to many estimative questions...good intelligence often reveals new uncertainties: as analysts gain information and improve their conceptual frameworks, they may identify additional possibilities that they had not previously considered. That should not be seen as a problem, since the goal of intelligence is to describe the uncertainty that surrounds a particular question, and not to eliminate or to reduce this uncertainty per se.<sup>51</sup>

Thus, ABI analysts of the future must learn to navigate comfortably within the complex and chaotic domains—discovering new uncertainties while eagerly embracing the “unknown unknowns.”

## CONCLUSION

A general should neglect no means of gaining information of the enemy’s movements, and, for this purpose, should make use of reconnaissances, spies, bodies of light troops commanded by capable officers, signals, and questioning deserters and prisoners. By multiplying the means of obtaining information, for no matter how imperfect and contradictory they may be, the truth may often be sifted from them.

—Baron Antoine-Henri Jomini<sup>52</sup>

The world has become a more complex place since September 11, 2001. Since then, the Intelligence Community has begun to adapt its processes and methodologies to address the complexities associated with a counterinsurgency campaign while providing this information to operational-level commanders and strategic-level decision-makers alike. Moreover, organizations such as NGA and the office of the Air Force Deputy Chief of Staff for ISR have paved the way for the adoption of the ABI methodology throughout the entirety of the IC. NGA’s NEA Cloud-computing architecture and its expertise in harnessing “Big Data” will become an integral part of the solution to address the data storage and interoperability challenges currently faced by DOD. Likewise, the Air Force will lead the way in transforming the ways and means of analysis and exploitation. This transformation is heralded throughout the service’s *Strategic Vision* document, noting that:

The most important and challenging part of our analysis and exploitation revolution is the need to shift to a new model of intelligence analysis and production. The growing complexity of the data we collect along with the sheer quantity of data has obviated the traditional linear model of production. The new model treats all intelligence collection as sources of meta-tagged data accessible across multiple domains...from which analysts—trained in all-source techniques and methods—can discover, assess, and create relevant knowledge for commanders and decision makers at all levels.<sup>53</sup>

Thus, the stage is set to transform the ways and means of today’s analytical processes and methodologies. Likewise, this analytical paradigm shift rests squarely atop the foundation of ABI methodology—framed by an improved and adopted tradecraft that will soon bolster the entirety of the IC with better and more capable analysts.

## Glossary

**Activity-Based Intelligence.** A discipline of intelligence where the analysis and subsequent collection are focused on the activity and transactions associated with an entity, a population, or an area of interest. (see Endnote 34)

**Cynefin Framework.** A decision-making or analytical framework that recognizes the causal differences which exist between system types and proposes new approaches to decision-making in complex social environments. (see Endnote 25)

**Geospatial Intelligence.** The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. Also called GEOINT. (JP 1-02. SOURCE: JP 2-03)

**Human Intelligence.** A category of intelligence derived from information collected and provided by human sources. Also called HUMINT. (JP 1-02. SOURCE: JP 2-0)

**Intelligence.** 1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities. (Approved for incorporation into JP 1-02)

**Intelligence Community.** All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. Also called IC. (Approved for incorporation into JP 1-02 with JP 2-0 as the source JP)

**Intelligence Discipline.** A well-defined area of intelligence planning, collection, processing, exploitation, analysis, and reporting using a specific category of technical or human resources. (Approved for incorporation into JP 1-02)

**Intelligence Production.** The integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence for known or anticipated military and related national security consumer requirements. (Approved for inclusion in JP 1-02)

**Signals Intelligence.** 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called SIGINT. (JP 1-02. SOURCE: JP 2-0)

## NOTES

<sup>1</sup>Clay Dillow, "Can Technology Save the Military from a Data Deluge?" *Popular Science*, 2 November 2011, <http://www.popsoci.com/technology/article/2011-11/can-technology-save-military-its-technology>.

<sup>2</sup>National Security Strategy, under *Strengthening National Capacity—A Whole of Government Approach* (May 2010), 15.

<sup>3</sup>U.S. Government Accountability Office, *Actions Are Needed to Increase Integration and Efficiencies of DOD's ISR Enterprise* (2011).

<sup>4</sup>House Permanent Select Committee on Intelligence, *Performance Audit of Department of Defense Intelligence, Surveillance, and Reconnaissance*, Executive Summary (April 2012), ii.

<sup>5</sup>Ibid.

<sup>6</sup>Col Jason M. Brown, "Strategy for Intelligence, Surveillance, and Reconnaissance," Research Report (Maxwell AFB, AL: Air War College, 14 February 2013), 24.

<sup>7</sup>House Permanent Select Committee on Intelligence, ii.

<sup>8</sup>For specific information pertaining to the success of intelligence operations in Iraq, see LTG Thomas F. Metz, COL William J. Tait, Jr., and MAJ J. Michael McNealy's article, "OIF II: Intelligence Leads Successful Counterinsurgency Operations," in *Military Intelligence Professional Bulletin* 34-05-3 (Fort Huachuca, AZ: U.S. Army Intelligence Center of Excellence, July-September 2005), [https://www.fas.org/irp/agency/army/mipb/2005\\_03.pdf](https://www.fas.org/irp/agency/army/mipb/2005_03.pdf).

<sup>9</sup>MG Michael T. Flynn, Capt Matt Pottinger, and Paul D. Batchelor, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Center for a New American Security, January 2010, <http://www.cnas.org/media-and-events/press-release/fixing-intel-a-blueprint-for-making-intelligence-relevant-in-afghanistan>, 11.

<sup>10</sup>Ibid., 21.

<sup>11</sup>Ibid., 4.

<sup>12</sup>Ibid., 8.

<sup>13</sup>Ibid.

<sup>14</sup>This definition is proposed in a Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance White Paper, "Revolutionizing AF Intelligence Analysis," dated January 2014. This definition synchronizes with a current Defense Intelligence Agency proposal for the definition of an analyst as "one who synthesizes information from one or more sources through processing, exploitation, or analysis to produce intelligence to inform or to provide decision advantage for defense or national policymakers" (ODNI Analyst/Collector Count Briefing, October 2013).

<sup>15</sup>Gregory F. Treverton and C. Bryan Gabbard, *Assessing the Tradecraft of Intelligence Analysis*, RAND Technical Report TR-293 (Santa Monica, CA: RAND, 2008), 1.

<sup>16</sup>Ibid., 7.

<sup>17</sup>Ibid.

<sup>18</sup> Ibid.

<sup>19</sup> David J. Snowden, *The Cynefin Framework* (YouTube, The CognitiveEdge Network, uploaded 11 July 2010), <http://www.youtube.com/watch?v=N7oz366X0-8>.

<sup>20</sup> Ibid.

<sup>21</sup> Treverton and Gabbard, *Assessing the Tradecraft*, 1.

<sup>22</sup> David J. Snowden and Mary E. Boone, "A Leader's Framework for Decision Making," *Harvard Business Review*, November 2007, 1.

<sup>23</sup> Ibid.

<sup>24</sup> Ibid.

<sup>25</sup> Snowden, *The Cynefin Framework*.

<sup>26</sup> Ibid.

<sup>27</sup> Ibid.

<sup>28</sup> Snowden and Boone, "A Leader's Framework," 5.

<sup>29</sup> Gregory F. Treverton, "Intelligence for an Age of Terror"; Mark Phillips, "A Brief Overview of Activity Based Intelligence and Human Domain Analytics" (paper approved for release by National Geospatial-Intelligence Agency, 28 September 2012), 2.

<sup>30</sup> Ibid.

<sup>31</sup> Ibid.

<sup>32</sup> Gregory F. Treverton, *CIA Support to Policymakers: The 2007 National Intelligence Estimate on Iran's Nuclear Intentions and Capabilities* (Washington, DC: Central Intelligence Agency Center for the Study of Intelligence Lessons Learned Program, May 2013), 27.

<sup>33</sup> Ibid.

<sup>34</sup> Mark Phillips, "A Brief Overview of Activity Based Intelligence and Human Domain Analytics," *Trajectory Magazine*, 28 September 2012, <http://trajectorymagazine.com/web-exclusives/item/1369-human-domain-analytics.html>.

<sup>35</sup> Ibid.

<sup>36</sup> United States Geospatial Intelligence Foundation, "Activity Based Intelligence" (working paper, Activity Based Intelligence Working Group, 29 November 2012).

<sup>37</sup> Gabriel Miller, "Activity-Based Intelligence Uses Metadata to Map Adversary Networks," *C4ISR Journal* (8 July 2013), <http://www.defensenews.com/article/20130708/C4ISR02/307010020/>.

<sup>38</sup> Ibid.

<sup>39</sup> Ibid.

<sup>40</sup> Ibid.

<sup>41</sup> Ibid.

<sup>42</sup> Keith L. Barber, "NSG Expeditionary Architecture: Harnessing Big Data," *Pathfinder: National Geospatial-Intelligence Agency Magazine* 10, no. 5 (September/October 2012): 8, <https://www1.nga.mil/MEDIAROOM/PATHFINDER/Pages/default.aspx>.

<sup>43</sup> Ibid.

<sup>44</sup> Col Jill E. Singleton, "Data Integration: Charting a Path Forward to 2035," Research Report (Maxwell AFB, AL: Air War College, 14 February 2011), 4.

<sup>45</sup> Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," Special Publication 800-145 (Gaithersburg, MD: U.S. Department of Commerce, September 2011): 2, <http://csrc.nist.gov/publications/PubsSPs.html#800-145>.

<sup>46</sup> Barber, "NSG Expeditionary Architecture," 3.

<sup>47</sup> Defense Acquisitions, Report to the Chairman, Committee on Armed Services, House of Representatives, *Steps Needed to Ensure Interoperability of Systems that Process Intelligence*

*Data*, GAO-03-329 (Washington, DC: General Accountability Office, 2003): 4, <http://gao.gov/products/GAO-03-329>.

<sup>48</sup> Ibid.

<sup>49</sup> Barber, "NSG Expeditionary Architecture," 4.

<sup>50</sup> RAND, "Assessing the Tradecraft," 38.

<sup>51</sup> Jeffrey A. Friedman and Richard Zechkhauser, "Assessing Uncertainty in Intelligence," *Intelligence and National Security* 27, no. 6 (December 2012): 826.

<sup>52</sup> Baron Antoine-Henri Jomini, *The Art of War*, trans. Capt G.H. Mendell and Lt W.P. Craighill (Gutenberg eBook #13549, 28 September 2004), 273.

<sup>53</sup> Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance, "Air Force ISR 2023: Delivering Decision Advantage" (Washington, DC: 2013), 13.

<sup>54</sup> Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: 15 January 2014), [http://www.dtic.mil/doctrine/dod\\_dictionary/](http://www.dtic.mil/doctrine/dod_dictionary/).

*Colonel James L. Lawrence II is commander of the 693rd Intelligence, Surveillance, and Reconnaissance Group (Distributed Ground Station-4) headquartered at Ramstein Air Base, Germany. He is a 1993 graduate of Fayetteville State University with a BA degree in English Language and Literature. Additionally, in 2007 he earned an MSSI degree from the then-National Defense Intelligence College (now NIU) and in 2014 a Master of Strategic Studies degree (with Academic Distinction) from the Air War College. The basis for this AIJ article is his AWC professional studies paper of the same title, which was nominated for the College's Military Operations Outstanding Research Award. Colonel Lawrence's most recent operational assignments include serving as U.S. Air Forces Central Command (AFCENT) Deputy Director of Intelligence at Al-Udeid Airbase, Qatar, in support of operations in Iraq, Afghanistan, and the Horn of Africa. He commanded the 48th Intelligence Squadron (Distributed Ground Station-2) at Beale AFB, CA, and served as Director of Operations for the 30<sup>th</sup> Intelligence Squadron (Distributed Ground Station-1) at Joint Base Langley-Eustis, VA.*



---

# Is Intelligence an Instrument of National Power?

by Dr. Adrian Wolfberg and CDR (USN) Brian A. Young

---

No one would dispute that intelligence is vitally important to preserving the security of the United States against state or non-state actors—foreign or domestic—just as no one would dispute that knowledge is power. Yet, there is wide disagreement over the role of intelligence in the realm of strategic thinking: Is it an instrument of national power or an enabler of national power? The dispute persists because as a national security community we have not defined what we mean by the term “instrument,” which has allowed national security stakeholders to advocate inconsistent roles for intelligence. We view the debate not as an abstract exercise but one that exposes the core difference between the hopes and the realities of intelligence. We propose that a political problem exists when we want intelligence to be an instrument because, in so doing, we not only misunderstand its nature; we generate a second-order effect of diminishing its ability to speak truth to power.

## DIFFERING VIEWPOINTS

Those who argue that intelligence is an instrument of national power use the underlying metaphor of “knowledge is power” as it should be applied by a policymaker against a recipient—the threat—in the same way a hammer is used against a nail. Those who argue it is not an instrument, while they agree knowledge is powerful, focus on the role of intelligence role in supporting the source of the power—the policymaker—to help figure out when, where, or how much to use a hammer. The dilemma these perspectives create is a contradictory view of how intelligence is conceptualized: Intelligence as an instrument implies that policy shapes knowledge whereas intelligence as an enabler implies knowledge shapes policy. We argue for the latter case and it excludes the former. Not only does knowledge shape policy (and operations), but the truthfulness of knowledge offered by intelligence officers to policymakers must never be shaped by policy.

Doctrine, as we discuss below, defines intelligence as information that has been collected and analyzed into knowledge specifically for supporting policymaker decision-making. There are exceptions to this definition, the most prominent being covert action. Even though covert action—

such as paramilitary activity to capture, kill, or sabotage—is part of the mission of the Central Intelligence Agency, national security doctrine omits it from its meaning of the term “intelligence.” We suggest the reason why is that covert action is a military-like action taken after a political decision has been made to achieve policy objectives authorized by the President. As such, while it is clear to us that covert action uses force against a foreign threat, it is a completely different phenomenon from the creation of knowledge.

## WHAT DOCTRINE SAYS

National security doctrine published over the past 20 years, when including the term “intelligence,” describes it as the collection and analysis of information—i.e., knowledge creation—regardless of whether intelligence is included in the doctrine as an instrument or not. Where doctrine has included intelligence as an instrument of national power, it has been almost exclusively counterterrorism-related. Its inclusion as an instrument emerged after the terrorist attacks of 2001, began to be downplayed beginning in 2010, and has been largely removed since 2011. In our review of national security doctrine over the past 20 years, we included those publications in which at least two instruments were mentioned. A number of military-related strategies, such as the 2012 *Sustaining U.S. Global Leadership: Priorities for the 21<sup>st</sup> Century Defense*, refer to other instruments but do not specify what they are; hence, these documents were not considered in our analysis. More importantly, in no document was the word “instrument” actually defined other than the listing and definition of specific instruments such as military, diplomatic, and so on.

From 1994 through 2000, the White House published its annual *National Security Strategy*. In each of these seven documents, the word “instruments” was used to include the use of military, diplomatic, and economic actions as the means to implement strategy. Intelligence was mentioned in the 1998 and 1999 strategies insofar as it supported these means, and intelligence was described in these two strategies as the collection and analysis of information.



From 2002 through 2010, national security doctrine included intelligence and named it specifically as an instrument except in a number of cases discussed below where “tool” was used, but each document described intelligence as collection and analysis of information. Intelligence as an instrument first emerged in the White House’s 2002 *National Security Strategy* in the section discussing terrorism, and then in its 2003 *National Strategy for Combating Terrorism* where it identified intelligence as a tool, using it synonymously as an instrument, along with other tools such as the military, diplomacy, and so on.

Congress passed into law the *Intelligence Reform and Terrorism Prevention Act of 2004*, in which it described the National Counterterrorism Center as integrating intelligence as one of the instruments of national power. The Joint Chiefs of Staff published its *National Military Strategic Plan for the War on Terrorism* in 2006 and included intelligence as an instrument of national power. The White House published *The National Security Strategy of the United States* in 2006, listing intelligence along with the military and diplomacy instruments for fighting terrorism, and the *National Strategy for Combating Terrorism* also in 2006, including intelligence as an instrument of national power. However, then we start to see a shift in how intelligence is framed in the White House’s 2010 *National Security Strategy*, in which intelligence is included as an instrument of national power although not in the context of counterterrorism, but rather in the broader American engagement in the global arena. Similarly, a broader engagement for intelligence is used by the Department of Defense’s *Quadrennial Defense Review* published in 2010 that included intelligence as an instrument of national power.

---

***The Department of Defense’s 2014 Quadrennial Defense Review did include intelligence as a tool of national power but only in the section pertaining to counterterrorism.***

---

The Joint Chiefs of Staff published the *National Military Strategy* in 2011 but excluded the mention of intelligence as an instrument of national power, mentioning only the military, diplomatic, and economic instruments. The JCS also published in 2011 the *Joint Operations* (JP 3-0) and *Joint Operations Planning* (JP 5-0) doctrines, neither of which included intelligence as an instrument of national power, mentioning only the military, diplomatic, economic, and information. The White House published the *National Strategy for Counterterrorism* in 2011, which also excluded intelligence as a tool of American power.

More recently, in 2013 the JCS published its *Doctrine for the Armed Forces of the United States* (JP-1) and *Multinational Operations* (JP 3-16), which excluded intelligence as an instrument of national power, instead identifying the military, diplomatic, economic, and information as the instruments. The Department of Defense’s 2014 *Quadrennial Defense Review* did include intelligence as a tool of national power but only in the section pertaining to counterterrorism. Lastly, the White House published its 2015 *National Security Strategy*, which did not include intelligence as an instrument of national power; it did make the point that intelligence plays a support role to assist instruments.

## WHAT ARE INSTRUMENTS?

To help move us in the direction of defining the term “instruments,” we next consider the characteristics of instruments as the term has been used in the doctrine discussed above. We use as a baseline the specific instruments mentioned during the pre-2001 and post-2010 time periods when instruments included the military, diplomatic, economic, and, for the most part, information. By doing so, we are able to compare these instruments in order to determine what commonalities exist. Then we evaluate intelligence with respect to these commonalities in order to determine the degree to which the concept of intelligence is consistent with the baseline use of instruments. Three characteristics are considered. First, how is the instrument wielded? Second, who wields the instrument against whom? Third, can the instrument be used independently from the others?

## HOW IS THE INSTRUMENT WIELDED?

How are the instruments wielded? What are the mechanisms of effect? To explain these questions the following analogy is used. Two weapons of ancient combat are the spear and the shield. The spear is used primarily to project power toward an opponent in order to weaken or otherwise cause the opponent to react in a certain way. The shield, on the other hand, is primarily used in a more defensive way in order to protect one’s ability to continue to project power and act more freely in light of the opponent’s moves. This is not to say that a spear cannot be used defensively or a shield cannot be used offensively, or that they cannot be used together. It is only to say that each instrument is designed primarily in a particular way.

The Department of State—as lead agency—uses diplomacy through negotiations with global actors as a way of avoiding armed conflict. The United States maintains open relations with most other nations and actively seeks, through near-continuous negotiation, to convince others to act in a way that is consistent with its national objectives. In order to do this, the Department of State actively engages on the

international stage in a variety of ways ranging from multilateral talks on specific issues to daily one-on-one bilateral engagements with individual nations. In this sense, diplomacy is like a spear. It is used to project power actively in order to convince others to act in a certain way. However, diplomacy is also used to bolster the use of international institutions. Consequently, in this sense it is like a shield, developing capabilities that protect U.S. and allies' interests.

Informational power refers to the ability to communicate with and message to the world. Not only the Department of State but others in the U.S. government are involved with strategic communications, the messaging of what the United States wants the foreign public to understand. This is accomplished primarily through public diplomacy transmitting content through traditional media as well as online. The point of this effort is to affect the world's opinion of the United States. This is done actively in order to shift attitudes, hopefully leading to the modification of behaviors. The Department of State and others identify what opinion of the United States is needed from foreign publics to advance American interests. In this way, information power is actively wielded to project power like a spear as it is thrown toward the foreign actors in full view.

Military power, it seems logical to assume based by its violent capability, would also be actively projected. This is true in the obvious sense that if militaries are ostensibly used to kill and break things, and if a potential adversary does not want to risk having its people killed and its things broken, it will be inclined to behave in a certain way. This is, of course, not the only use for militaries. Military power of the United States usually causes potential adversaries to be hesitant of provoking the ire of the United States for fear of the response. In this way the military is a shield. It protects our freedom to act as we choose. It is arguable which is the primary function of the military, offense or defense. However, as either a spear or a shield, the military is used actively to project power or enable the ability to project power via other instruments.

Defining the economic instrument of power is something of a challenge. For our purposes the economic instrument is defined as actions taken—some as punishment, others as rewards—in the international arena to include sanctions, foreign aid, and establishment of trade policies. We impose or lift sanctions, offer or withhold aid, and modify our trade policies in order to influence the activities of every nation with which we have economic ties. It is clear that economic power is wielded like the spear. It is arguable whether trade policies could be used defensively to protect or prevent the likelihood of wars between trading partners. The economic instrument is viewed as primarily designed to project power actively though it too can be used defensively.

---

### ***Intelligence is a critical enabler of diplomatic, informational, military, and economic power projection.***

---

If we consider intelligence as we just have as an instrument, we effectively are asking the question, “Does the United States use intelligence to directly—offensively or defensively—influence the activities of others in a way that is consistent with our desires?” There is no question that intelligence is used, but intelligence products are not themselves the tools directly causing the adversary to act in a certain way. Intelligence is a critical enabler of diplomatic, informational, military, and economic power projection. Intelligence products themselves are not used directly; rather they inform the source of power serving to adjust, in a sense, how much, where, and when national power should be exercised. In this way, the character of intelligence is unlike the other instruments of national power.

#### **Who Wields the Instrument Against Whom?**

We next consider who determines the use of each instrument and who the intended target is. For example, who wields the diplomatic power? Historically, the President of the United States has set diplomatic policy implemented through the Secretary of State. Other government actors may get involved or try to get involved, but ultimately it is up to the President to set the direction of diplomacy, deal with the consequences, and communicate the results to the American people. This is not to say that the Congress, the public, the media, and others in government do not have a say, only that the President has the responsibility for developing and executing the policies. In that sense, the President wields diplomatic power.

Who wields informational power? Until the explosion of the Internet, the message that the United States projected to the world was based primarily upon official positions set forth by the White House. Those positions were influenced by a number of social and political factors and the media played a large role, but they were ultimately the responsibility of the President. Nevertheless, it is fair to say that today the world has significantly more information available to it, and its ability to access it has increased with the growth of Internet connectivity. Additional information includes everything from media reports of current events to social media. This makes the answer to the question “Who wields information power?” very difficult to answer with any real certainty. Ultimately, several groups exercise control of the message sent to the

world with regard to the United States: the President, the media, and the American public. On the other hand, no one has control over the Internet. It is often hard to figure out who is pulling the lever behind the face of information.

Who wields military power? The President of the United States is the commander and chief of the American military. In that role the President directly wields military power and is limited only by the Constitution, funding from Congress, and public opinion. Who wields economic power? As before, the economic instrument is defined to mean sanctions, foreign aid, and establishment of trade policies. This definition leads to the conclusion that the President and the Congress both wield economic power.

Who is the intended recipient of diplomatic, informational, military, and economic instruments? While the desired outcome is going to be different for each instrument, the type of targeted recipient is the same. In other words, the instrument's outcome may seek to sway an adversary's public opinion, affect internal political discussions, affect commercial and business sectors, their relations with neighbors and trading partners, or any combination of these and a host of others. However, in each case Americans who wield instruments of national power ultimately do so in order to influence those who have the power and authority to cause the actions we desire. These instruments seek to affect an adversary's decision-maker.

Who wields intelligence? The President ultimately sets priorities. Congress provides funding. Still, neither of these really answers the question in the sense that it was answered for the other instruments of national power. Executive decision-makers use intelligence in determining which policies or strategies would be most appropriate for a given situation. Diplomats use intelligence to determine the best way to proceed in a given situation. Intelligence is used to determine how the message being sent to the world is being interpreted. Military leaders use intelligence to determine how much risk to take in a particular situation, and where to apply resources to optimize military power. Intelligence is used to determine the effect or likely effect of sanctions, foreign aid, and establishment of trade policies. Intelligence is different from diplomatic, informational, military, and economic power in that anyone and everyone involved in execution of government missions uses it to inform policymakers, who then make use of it by shaping how and when to use their spears, shaping their instruments of power. Who is directly affected by the use of intelligence? American (and/or allied) policymakers are.

Diplomatic, informational, military, and economic powers have various groups who wield them. What those sources of power have in common is they wield the instruments directly at foreign actors to achieve a desired outcome. That is to say, the sources of these instruments of power—the holders

of the spear—interface and interact directly with others in the world. The sources of intelligence, on the other hand, are the collectors and analyzers of information, and use the resultant knowledge in order to advise American holders of power who then can take action by themselves or with the other instruments. Those limited few who wield instruments of power have the authority to engage with global actors. Those who wield intelligence do so ubiquitously but do not have such authority; their responsibility is to provide knowledge to those who do have the authority. In these ways, the character of intelligence is unlike the other instruments of national power.

### **Can the Instrument Be Used Independently?**

The motivation for this question is based on the assumption that the world is very complex and that bureaucratic divisions within government or any organization can never so neatly contain the framing of a problem, the selection of a solution, or its implementation. Since we live in an interdependent world where actions cause other actions, we assume an instrument cannot be employed without considering other instruments.

We propose that informational power requires two things to wield effectively: integrity and reach. Other instruments reinforce integrity if they demonstrate that "we do what we say." Communicating the message does not require the use of diplomatic, military, or economic power; it only requires that when we do use diplomatic, military, or economic power to communicate the message the source of power is consistent with the message that we communicate. Reach in this context is expanding the range of recipients by increasing the use of the sources of power; greater reach creates greater risk, especially when the integrity of the message by other sources of power cannot be managed effectively, which is typically the case. The longer the duration of use the more dependent information power becomes on the other instruments of power, and the more difficult integrity and reach are able to maintain.

Military, diplomatic, and economic powers follow the same interdependent logic. Each can be used only in the short term to a specific end, but not in isolation over the long term. The mere threat of the U.S. military engaging in an area may be enough for coercive diplomacy to get all but the staunchest or hard-to-isolate potential adversary to take notice and change its behavior. The actual use of military power eventually comes to an end and requires diplomatic and economic engagement. The use of economic tools has the same effect. Economic tools may be used within a diplomatic and informational strategy.

Intelligence is different. The knowledge created from the collection and analysis of information follows a logic of discovery, that of following the data and using analytic and

methodological techniques, employing various types of reasoning, confronting interpretation and bias issues, and ultimately delivering knowledge products to decision-makers regardless of how or who wields an instrument of power. While the world's behaviors and policymakers' concerns influence what topics intelligence pursues, the instruments of such sources of power do not affect knowledge production. Intelligence acts independently of the other instruments while the instruments of military, diplomacy, economics, and information are dependent upon each other. In this way, the character of intelligence is unlike the other instruments of national power.

## CONCLUSION

Intelligence as defined by national security doctrine over the past 20 years has consistently been stated as the collection and analysis of information leading to the creation of knowledge. For a period of about 10 years, seemingly triggered by the 9/11 terrorist attacks of 2001, primarily counterterrorism-related doctrine included intelligence as an instrument of national power in addition to the instruments of military, diplomatic, and economic power, informational power emerging in doctrine somewhat later. The effects of 9/11 likely motivated the sources of power to bring to bear enthusiastically everything this nation had to fight against the threat of terrorism, and in so doing broadened what we meant by an instrument of national power. Today, since at least 2011, doctrine for the most part has again narrowed its conceptualization of instruments to only those of military, diplomatic, economic, and informational. While likely no one event triggered this return, the WikiLeaks disclosure in 2010 of hundreds of thousands of classified documents—the largest in American history at the time—may have injected an incentive for reflecting on whether intelligence is an instrument of national power.

Is intelligence an instrument of national power? The answer is “no.” We used three lines of examination to explore the characteristics of an instrument, and compared intelligence to these characteristics. First, we argued that how an instrument is wielded is completely different among the military, diplomatic, economic, and informational instruments than with intelligence: the former set projects power while the latter enables sources of power. Second, we contended that who wields power and against whom they wield it are also completely different between these two sets of activities: instruments and enablers. Military, diplomatic, economic, and informational instruments are employed by a very limited few who have the authority to project power in order to affect actors on the global stage, while intelligence is used ubiquitously without any knowledge producer having such authority to affect global actors. Rather, the intelligence is created in order to inform American policymakers and to enable the decisions they make.

Third, we concluded that interdependency between instruments is completely different: the use of military, diplomatic, economic, and informational instruments are highly dependent upon each other, whereas intelligence is employed relatively consistently regardless of the instruments of power it supports.

When we entertain intelligence—the collection and analysis of information leading to knowledge creation—as an instrument, we mistakenly give it a role as a power that can be projected onto the global arena. Covert action is an important instrument but it is not knowledge creation, i.e., intelligence. The risk in considering intelligence as an instrument is its absorption into the policymaking arena, an otherwise accepted and necessary relationship for an instrument of national power. However, the product of intelligence is truth, at least as we know it, and subjecting truth to power projection can result in very bad decision-making. A case in point is the manipulation of intelligence by policymakers between 2002 and 2003—specifically, by the Office of Special Plans within the Office of the Under Secretary of Defense for Policy—to find evidence of a link between terrorism and Iraq suggesting that Iraq had a weapon of mass destruction program. The risk in structurally bringing intelligence into the realm of policy as an instrument is that we lose sight of the real strength of intelligence as the ability to speak truth without political influence by those in authority, that is, to speak truth to power.

*Dr. Adrian Wolfberg is the Defense Intelligence Agency representative to the U.S. Army War College, and serves as its Chair for Defense Intelligence Studies. His recent DIA experience includes organizational policy, strategic planning, and change management, followed by a career in strategic and operational analysis ranging from support to the White House to state-level law enforcement agencies. Prior to joining DIA, he was a naval flight officer conducting SIGINT reconnaissance missions from carrier-based jet aircraft, and then was assigned to the Joint Staff J2 where he was an ELINT Indications and Warning officer. He holds a PhD in organizational learning (knowledge transfer) from Case Western Reserve University and is a graduate of the National War College. For additional information, Dr. Wolfberg can be reached by email at [adrian.wolfberg.civ@mail.mil](mailto:adrian.wolfberg.civ@mail.mil) or [awolfberg@gmail.com](mailto:awolfberg@gmail.com).*

*Commander (USN) Brian A. Young is a submarine officer and a 2015 graduate of the U.S. Army War College. He is assigned to Submarine Development Squadron FIVE in Silverdale, WA.*





---

# North Korea's Post-Totalitarian State:

## The Rise of the Suryong (Supreme Leader) and the Transfer of Charismatic Leadership

by Dr. (COL, USA, Ret) David W. Shin

---

[T]he ruling family, founded by Kim Il Sung, has brutalized its own population for half a century, murdering or starving to death some four million people. The Kims have squandered precious resources on a religious cult devoted to their own leadership while they have built palaces, swilled imported French cognac, and gifted their concubines with Swiss watches. Any such regime must be rated as highly unstable and combustible.<sup>1</sup>

— Jasper Becker

Many observers of North Korea may agree with Jasper Becker that the ruling Kim family of North Korea is an example of “how absolute power leads to evil and madness.”<sup>2</sup> According to Peter G. Northouse, Kim Jong-il, the son of Kim Il-sung, was the “classic example” of a coercive leader, along with Adolf Hitler and others, who “used power and restraint to force followers to engage in extreme behaviors.” Kim Jong-il’s coercive tools frequently involved the “use of threats, punishment, and negative reward schedules.” Northouse objects to coercive leaders because they are perceived to be selfish and ignore the “wants and needs of followers.” As a result, his definition of leadership suggests the right to be called a leader is only “reserved for those who influence a group of individuals toward a common goal” without the use of coercion.<sup>3</sup>

Not everyone seems to agree with Northouse’s understanding of leadership and the use of coercion, however. Joseph S. Nye, Jr., argues that, by and large, “those without formal authority tend to rely more on soft power, whereas those in formal positions are better placed to mix hard and soft power resources.” According to Nye, there are leaders who are able to attract followers with their “inherent qualities” and others who can persuade with their oratory skills. Still others possess charisma that attracts followers emotionally. On the other hand, leaders can use “threats and inducements” to coerce their followers.<sup>4</sup> This begs the question whether the Kims use coercive power only. Did Becker and Northouse fail to recognize the softer aspects of the Kims’ leadership?

Helen-Louise Hunter, a former CIA analyst, stated, “One cannot but be amazed at the overwhelming evidence of the people’s strong emotional attachment to Kim [Il-sung]. With all the instruments of control at their disposal, North Korea’s leaders could never have created so intense a psychological phenomenon had it not been for Kim’s own *unique* personality.”<sup>5</sup> Other knowledgeable observers of North Korea recognized there was “genuine belief held by the majority of the population in Kim’s greatness, benevolence and goodness” based on Korea’s neo-Confucian tradition. Kim enjoyed this popular support, in part, through monopoly control of information (and other totalitarian tools),<sup>6</sup> but one cannot ignore that “he had charisma... His talent of establishing a real rapport with ordinary people was at the centre of the Kim cult, however much this may have been manipulated and orchestrated for political ends.”<sup>7</sup>

North Koreans proclaimed Kim as the Father of the Nation<sup>8</sup> and fashioned a cult of personality unlike any other in the world that continues to deify him as the Supreme Leader (*Suryong*)<sup>9</sup> and eternal President.<sup>10</sup> Moreover, Andrei Lankov has recently argued that even Kim Il-sung’s son Kim Jong-il was “a *charismatic* politician and shrewd manipulator who eventually proved to be a match for his ruthless and street-smart father.”<sup>11</sup> These observations are a stark contrast to the common perception in the Western media that North Korea and its leaders are “bizarre” and “irrational, demonic, and self-destructive.”<sup>12</sup>

In short, the Kims appear to have been capable and charismatic leaders. This article presents an alternative view by evaluating the leadership styles of the first two Kims and considers what it may suggest for Kim Jong-un’s leadership development. It begins by briefly examining how Kim Il-sung consolidated his rule and softened Stalin’s totalitarian system to suit his own needs as the Supreme Leader of North Korea. Then it investigates a relatively obscure incident during Kim’s anti-Japanese guerrilla struggle that would shape and define him as a leader. Next, it examines Kim Il-sung’s leadership style and legitimacy and how they were transferred to his successors.

---

## KIM IL-SUNG'S MANIPULATION OF SOVIET TOTALITARIANISM AND DICTATORSHIP

After liberation from Japanese colonial rule in August 1945,<sup>13</sup> Kim Il-sung eventually manipulated the Soviet totalitarian system which consisted of six traits (dominant ideology, single mass party, terroristic police control, monopoly of information, control of the military, and central command of the economy)<sup>14</sup> to legitimize his charismatic rule as the Supreme Leader. When Kim returned from Manchuria after Korea's liberation from Japanese colonial rule, he believed he had more legitimacy to rule all of Korea as a former anti-Japanese guerrilla than the leaders of the South who were largely former Japanese collaborators.<sup>15</sup> His Manchurian experience taught him how to lead men under difficult conditions,<sup>16</sup> including subordinating himself and his men to the Chinese Communist Party (CCP).<sup>17</sup> Kim knew he was not allowed to fight for Korean independence until the CCP had defeated the Japanese,<sup>18</sup> and as a Korean even he would be vulnerable to accusations of being a pro-Japanese spy.<sup>19</sup> He would overcome the Chinese purge of the Minsaengdan (MSD), a pro-Japanese Korean group in Manchuria, to save an alleged group of MSD members. Consequently, they would form a special bond with Kim and remain loyal to him as they fought the Japanese<sup>20</sup> and returned to Korea after joining the Soviet Army in the Russian Far East (RFE).<sup>21</sup>

---

### *Kim seemed to know he needed both power and legitimacy.*

---

When Kim and his guerrillas arrived in North Korea, they contested for power with several factions to create a new nation under Soviet tutelage,<sup>22</sup> and eventually gained the upper hand as the other factions lacked their organization and leadership.<sup>23</sup> Some of Kim's comrades would die during the Korean War but those remaining continued to help him purge the others in the wake of war and consolidated their power as they rebuilt the country after the war.<sup>24</sup> The Soviet and Chinese factions eventually decided to challenge Kim's authority in 1956,<sup>25</sup> and he had to tolerate a joint intervention from Moscow and Beijing for a short period.<sup>26</sup> Eventually, though, he was able to purge most of his enemies by 1961.<sup>27</sup> The final opposition from the Kapsan faction (one of the domestic factions)<sup>28</sup> was eliminated in 1967.<sup>29</sup> Whenever the North faced difficulty, the regime invoked the symbolic arduous march of Kim's guerrillas in Manchuria to call on the people to follow those who sacrificed everything for the Korean revolution.<sup>30</sup>

In the end, Kim managed to create a totalitarian system with Korean characteristics, which softened the terroristic control

aspect of the Soviet system<sup>31</sup> with his cult of personality<sup>32</sup> mixed with elements of neo-Confucianism<sup>33</sup> and an ideology based on Korea's long desire to seek self-reliance and independence from foreign interference.<sup>34</sup> Kim seemed to know he needed both power and legitimacy. Kim appears to have started his "cult of personality" by 1956 to strengthen his legitimacy, but it intensified during the Chinese Cultural Revolution of the 1960s as the Chinese became more hostile to Kim and North Korea.<sup>35</sup> While he relied on his security services<sup>36</sup> and the Korean People's Army (KPA)<sup>37</sup> to maintain control of key institutions and the populace, he also had the charisma<sup>38</sup> to lead his people as the *Suryong* and depended on his trusted lieutenants to achieve his aims.<sup>39</sup> It is also true that, near the end of his rule, near-monopoly control of information began to weaken,<sup>40</sup> but he still managed to spread effective propaganda to counter it.<sup>41</sup> Kim also used education, various forms of art, and public activities to inculcate in his people how to live the life of a true revolutionary. North Koreans learned from books, movies, operas, and everyday life activities to become loyal revolutionaries of the Kim regime.<sup>42</sup> Furthermore, the Korean Workers' Party (KWP) served Kim as the single party comprised of a loyal core elite<sup>43</sup> coupled with his *Juche* ideology<sup>44</sup> that was easy for Koreans to understand after centuries of being subservient to China and their experience with Japanese colonialism. Kim's regime faced many challenges during his rule, but he appears to have earned the genuine admiration of his people and still "lives" as the eternal President.<sup>45</sup>

Kim also managed to achieve early economic success during the post-Korean War period with aid from the Socialist bloc,<sup>46</sup> but growth was unsustainable without reform. The economy began to decline in the 1970s. Pyongyang flirted with illicit activities in Europe<sup>47</sup> after its economic outreach to the West and Japan failed miserably<sup>48</sup> and Kim had to encourage everyone to earn hard currency by selling locally produced commodities.<sup>49</sup> In other words, he laid the foundation for "North Korea, Inc." in the 1970s, and his regime just barely managed to exercise its "command" of the economy until his death. Finally, one could argue Kim initially practiced positive transformational leadership but his promotion of the cult of personality and eventual collapse of the North Korean economy<sup>50</sup> degraded his leadership type to one of negative transformational and transactional leadership.<sup>51</sup> In spite of this, Kim did not rely on brute force only to survive and hold power. Without knowing Kim's relationship with his MSD guerrillas, it is difficult to understand how he could have managed to gain the admiration of his people. Hence, this study focuses on the MSD incident and how it became the defining moment for Kim Il-sung as the future leader of North Korea.

---

## THE ROLE OF THE MINSAENG DAN INCIDENT IN THE RISE OF KIM IL-SUNG

It is no secret that until the late 1990s the South Korean government banned the promulgation of the role of Kim Il-sung in the Korean Nationalist movement, and many historians in the West largely ignored the anti-Japanese Korean Communist movement in China.<sup>52</sup> According to Lim Un, a former colleague of Kim Il-sung who defected to the Soviet Union, many South Korean historians politicized the issue and refused to acknowledge Kim's anti-Japanese activities in Manchuria, alleging he was only a leader of "mounted bandits." Their aim was to accuse Kim of being a fraud to promote anti-Communism in South Korea. Lim confirmed he was the real Kim Il-sung, but denounced Kim's tyrannical rule and the lies he told about his activities in Manchuria to create the myth he was planning for the liberation of Korea in China while he was under Soviet protection in the RFE.<sup>53</sup> The point is, while Kim lied about his role during the liberation of Korea, he was a notable anti-Japanese guerrilla leader in Manchuria.

---

*While Kim lied about his role during the liberation of Korea, he was a notable anti-Japanese guerrilla leader in Manchuria.*

---

What is even less well-known about Kim Il-sung's activities in Manchuria is that the CCP almost executed him as it began to purge Koreans en masse during the early 1930s. The CCP suspected a group of pro-Japanese Koreans who established the MSD in February 1932 of being Japanese spies and launched its anti-MSD campaign from late 1932 to early 1935. This purge resulted in the killing of up to 2,000 Korean Communists and supporters.<sup>54</sup> However, what is the significance of the MSD experience for Kim Il-sung? According to Han Hong-koo, the CCP in Manchuria became so obsessed by the prospect of MSD agents it imagined 70 to 80 percent of Koreans living in the Kando base area in Manchuria were pro-Japanese agents.<sup>55</sup> By November 1933, several CCP cadres began to suspect Kim of being an MSD member.<sup>56</sup> Kim claimed he was accused of being a pro-Japanese agent because he aided the Chinese Nationalists in procuring materials for 500 uniforms with the help of a local landlord. Kim argued that without his help these Nationalist soldiers would have deserted or surrendered to the Japanese. He decided to help them because the Communist guerrillas may not have been able to establish and hold the guerrilla zones by themselves. The CCP reportedly accused Kim of "rightist capitulation" for helping the Chinese Nationalist army, not taking the anti-MSD campaign seriously, and allowing a sizable number

of MSD agents into the guerrilla army.<sup>57</sup> Han indicated that the CCP at this time was focused solely on the Chinese revolution, and any distraction to its revolutionary aims was not tolerated.<sup>58</sup>

Han argued that Kim was saved by Shi Zhongheng, a Chinese guerrilla commander whom Kim reportedly rescued during a combined guerrilla attack against the Japanese in the city of Dongning. Shi reportedly questioned how "a great Figure like Kim Il-sung could be a Japanese running dog and declared that if the CCP convicted him, then he would sever all his ties with the Communist guerrillas."<sup>59</sup> Additionally, "A [Chinese] Communist document praised Kim Il-sung, commenting that the besieged guerrillas could escape safely because of his 'composed, unwavering, adroit, and flexible leadership'" during the Dongning battle.<sup>60</sup> Since Shi was trusted by the CCP leadership in Manchuria, Kim was spared from the deadly purge.<sup>61</sup>

According to Han, for the North Korean leadership, the MSD purge is all about Korean nationalism and Kim's role in overcoming the Chinese tendency to protect their own revolution at the expense of Korean independence. The Chinese Communists declared "that the right of self-determination for the minority peoples in China could only be enjoyed after 'the final victory of the Chinese revolution and the complete expulsion of imperialist forces from China'."<sup>62</sup> This policy line was a problem for the Koreans in the CCP since the Chinese made it clear that they would not tolerate Koreans pursuing anti-Japanese activities "only for the sake of the Korean revolution."<sup>63</sup> As a result, it is not surprising Armstrong argued that "the fact Kim fought under Chinese command and was himself a member of the CCP disappeared from North Korean histories after the Korean War."<sup>64</sup> Despite this assertion, Kim disclosed in his memoir that, during the winter of 1931, he established contact with the CCP for the first time and "became a cadre of an organization of the Chinese party," continuing his "relations with the Chinese Communist Party throughout the whole period of the anti-Japanese armed struggle."<sup>65</sup> The fact that well over 90% of CCP members in east Manchuria were Koreans may have comforted the Korean Communists since they were essentially playing a leading role in the local party anyway.<sup>66</sup>

Han argues that the two most important lessons from the MSD purge are how it shaped the *Juche* ideology and idealized the unique relationship between the North Korean leader and his people.<sup>67</sup> Han also emphasized that "the greatest significance in studying the MSD Incident lies in its long-lasting influence on North Korea and its 'Great Leader' Kim Il-sung."<sup>68</sup> Han stressed the MSD incident is critical to Kim because it led him to the band of loyal guerrillas and orphans who would eventually follow him to Korea after liberation.<sup>69</sup> In fact, it is likely that only about 30-40 of his



guerrillas had experienced the MSD purges out of approximately 100 guerrillas who returned to Korea with him after Japan's surrender. The other 60-70 guerrillas were from elsewhere in Manchuria or had joined the unit after the MSD purges. Han argues these MSD guerrillas formed the core leadership of Kim's regime which "was strong enough to shape the basic configuration of north Korean political culture."<sup>70</sup>



**Figure 1.** North Korean painting of Kim Il-sung with alleged MSD agents at Mount Maan and Kim directing the burning of the CCP files that tainted them as pro-Japanese agents, <http://search.aol.com/aol/image?it=sb-top&v t=webmail-searchbox&q=north+korean+paintings>.

The point is that, if one ignores or is unaware of the significance of the MSD incident in Kim's leadership development, it is likely then to have an impact on the overall judgment about Kim, his leadership ability, and his subsequent actions in North Korea. The story of Kim and his MSD guerrillas began when he became the Third Division Commander of the Second Army, NEAJUA, in early March 1936.<sup>71</sup> When Kim marched to Mount Maan with a small band of guerrillas to link up with a part of his command, he discovered the unit had not arrived. The only option he had to form the unit was a band of about 100 MSD suspects.<sup>72</sup> One of Kim's hagiographies highlighted his "motherly affection" for the MSD suspects and claimed he viewed them as "the most valuable thing in the world." When errors were committed against them, he worked tirelessly to rectify them with deep concern. Kim "loved and trusted them" and cultivated them to become "indomitable Communists through education and actual struggles."<sup>73</sup>

According to Han, Kim reviewed the records of the MSD suspects and decided to give them all a second chance. He reportedly ordered some of them to burn all the files that had tainted them at some risk to his own well-being and, needless to say, all of them broke down in tears (see Figure 1). Han writes, "The flames and the wailing symbolized the starting point of the unique relationship between Kim Il-

sung and his followers that lasted almost six decades."<sup>74</sup> These MSD suspects participated in the Bocheonbo raid against the Japanese that would bring Kim fame.<sup>75</sup> Most importantly, Han argues the MSD incident forced Kim to contemplate the issue of an independent Korean revolution, thus planting the seed of *Juche* ideology and shaping the formation of his relationship with the masses in North Korea.<sup>76</sup>

Thus, the Kim family's right to lead all of Korea begins with this anti-Japanese legacy since Kim knew how most Koreans on both sides of the Demilitarized Zone felt about the Japanese, and he manipulated this popular belief to indoctrinate those in the North that they were the true Koreans while pro-Japanese Koreans and the U.S. imperialists were exploiting the masses in the South. This narrative probably resonated in the South as well since many viewed the government in Seoul as undemocratic at the time. According to John Tirman, the U.S. government was aware President Syngman Rhee was "a demagogue 'bent on autocratic rule'." Moreover, Rhee was reportedly chosen over other Korean leaders in the South because the hard-right wing was largely perceived as Japanese collaborators.<sup>77</sup> This kind of sentiment probably convinced Kim that most South Koreans preferred an anti-Japanese and independent Nationalist government—his own regime in the North. Having said that, what else do we know about Kim's leadership credentials?

## KIM IL-SUNG'S LEADERSHIP STYLE AND LEGITIMACY

**K**im Il-sung appears to have understood that force and legitimacy were both key sources of power and that they have a relationship—"force without legitimacy brings chaos; legitimacy without force will be overthrown."<sup>78</sup> There seems to be near consensus that Kim ultimately enjoyed loyalty from the regime's key institutions and the people, but what kind of legitimacy did he have? According to the noted social scientist Max Weber, the discussion of legitimacy begins by first defining the concept of "authority." Weber defines authority as "the probability that a specific command will be obeyed." Moreover, authority that is obeyed for pure interest (pragmatic calculus), mere custom (habitual behavior), or mere affect (personal devotion of the follower) is judged to be relatively unstable.<sup>79</sup> What is required for stability is legitimacy and there are three kinds of legitimate authority.

The first is legal authority, the purest type being based on the bureaucracy, and the people obey the rules and regulations, to include the person in authority.<sup>80</sup> In 1948 North Korea promulgated its first constitution and drew significantly from the constitutional traditions of the Soviets. For instance, it granted rights to the country's ethnic



minorities even though nearly all of its citizens were Koreans. At the same time, there were many factions vying for power and the KWP made concessions such as allowing private ownership of property and businesses. It also “granted a long series of guaranteed rights and privileges to citizens, such as freedom of speech, the right to religious practice, and the right to be free from arbitrary arrest and detention.” However, it was only a matter of time before the constitution was subordinated to the KWP as Kim consolidated his power. This reality was revealed when the North revised its constitution in 1972. *Juche* became the state’s guiding ideology and elements that were borrowed from the Soviets were omitted from the revised version. Kim also became the first (and only) President of North Korea and it was evident he was “accountable to no one.”<sup>81</sup> Although one could argue this indicated that Kim used legal authority to legitimize his rule, he was clearly above the laws and regulations as the Supreme Leader. In other words, while he did not ignore the concept of legal authority, it is safe to say this is not how he derived his true authority and legitimacy.

In the second case of legitimacy, the focus is on traditional authority with the purest type being patriarchal authority. It upholds the belief in the old social order and tradition, and the people “are completely and personally dependent on the lord.” Even the system’s administrators are completely dependent on the ruler and, as a result, the ruler can indiscriminately exercise his authority. Weber noted that “sultanistic rule” represented the extreme form of patriarchal authority type,<sup>82</sup> and Juan Linz and Alfred Stepan argued that Kim Il-sung was one of the few modern sultanistic rulers.<sup>83</sup> However, Linz and Stepan also suggested that sultanistic rule is not a form of totalitarian rule since it does not have a ruling ideology.<sup>84</sup> As a result, since *Juche* is the guiding ideology in the North, sultanistic rule should be ruled out, while patriarchal authority seems to describe how Kim eventually exercised his legitimacy.

The final type of legitimacy is charismatic authority, in which the adoration of the people to the ruler and the ruler’s “gifts of grace (charisma)” form the base of legitimacy. The purest form includes “the rule of the prophet, the warrior hero, [and] the great demagogue.” The ruler is usually referred to as the leader and is followed by the disciple. The followers obey the ruler for his exceptional qualities and they remain loyal as long as the ruler’s charisma is “proven by evidence.” In short, if the charismatic ruler loses heroic strength or the people lose faith in the ruler’s leadership ability, the ruler’s reign would end. The ruler must achieve success or his authority may weaken. Furthermore, the system’s administrators are selected based on their own charisma and personal loyalty to the ruler, and not on any special qualification. This is crucial since the system’s success depends on the unity of the ruler and his administrators.<sup>85</sup>

---

***Kim relied on his anti-Japanese legacy to legitimize his rule and used the totalitarian system to ensure near-monopoly control of information. He was not afraid to use coercive power to maintain control and to eliminate his enemies...***

---

The concept of charisma appears to be a valid concept for analyzing the Kim family’s leadership. This is particularly true when one recognizes that Weber’s discussion of charisma was insightful enough to foresee the problem of leadership succession and how it would evolve during transitions of leadership. He noted that one way is for the charismatic leader to select his successor and gain the support of his religious or military elite. Sometimes this could lead to “hereditary charisma,” in which the essential qualification is the blood ties to the leader.<sup>86</sup> In the end, both patriarchal and charismatic authority offer a valid form of legitimacy for Kim Il-sung, but legal authority seems less relevant even though it was not completely ignored. This leads to a discussion about power, which Nye admits is “a contested concept,” but defines it as “the ability to alter others’ behavior to produce preferred outcomes.”<sup>87</sup>

According to Bryan Watters, there are many ways to obtain and exercise power: (1) reward power (i.e., rewarding followers for compliance),<sup>88</sup> (2) coercive power (i.e., obtaining compliance with threats), (3) legitimate power (discussed above), (4) referent power (i.e., “trusted and respected” by others), (5) expert power (i.e., derived from “experiences, skills or knowledge”), (6) information power (e.g., those in charge possess “needed or wanted information” to gain temporary advantage),<sup>89</sup> (7) position power (i.e., combination of legitimate, reward, and punishment powers), (8) personal power (i.e., derived from combination of expert and referent powers), (9) remunerative power (i.e., offering of material rewards), and (10) normative power (i.e., offering of symbolic rewards).<sup>90</sup> As shown above, despite the totalitarian character of the regime, the story of Kim Il-sung’s rise and consolidation of power indicates that, like many other leaders, he probably used all of these ways to gain and wield power during his rule.

For instance, Kim relied on his anti-Japanese legacy to legitimize his rule and used the totalitarian system to ensure near-monopoly control of information. He was not afraid to use coercive power to maintain control and to eliminate his enemies, but he also used a combination of reward, referent, and positional power by effectively employing his propaganda organs to establish a cult of personality that appealed to the Korean people’s desire for independence

from foreign domination. In spite of this, Daniel Chirot argued that Kim was a tyrant because he attempted to “control all thought” of his people by portraying himself as a “Confucian sage.” If Kim truly believed in his legitimacy to rule, it would not have been necessary to manufacture his cult of personality. The fact he did so “proved Kim lacked the support of his people similar to other tyrannies.” Nevertheless, Chirot admitted, “It is much harder to tell what people really think in North Korea” because it is so isolated from the outside world.<sup>91</sup> As discussed earlier, former CIA analyst Helen-Louise Hunter concluded Kim used his charisma to connect with the people, which implied he was not a mere tyrant in the traditional sense. If so, what kind of leadership style did he have?

According to Peter Northouse, “One of the more widely recognized approaches to leadership is the situational approach,” which suggests “different situations demand different kind of leadership.” In other words, to be an effective leader one must be capable of adapting “his or her style to the demands of different situations.”<sup>92</sup> Thus, the situational approach includes four different leadership styles that attempt to identify “the behavior patterns of a person who attempts to influence others.” They include directing (i.e., focusing on giving “instructions about what and how goals are to be achieved” by followers and providing careful supervision), coaching (i.e., focusing on directing as well as encouraging followers and eliciting their input), supporting (i.e., a goal is important but it “gives subordinates control of day-to-day decisions” while the leader is available to help solve problems), and delegating (i.e., focuses on letting “subordinates take responsibility for getting the job done the way they see fit”).<sup>93</sup> The fact that Kim Jong-il was able to establish a monolithic guidance system to control his party elites by 1973<sup>94</sup> suggests Kim Il-sung probably had delegated some authority to his son by the early 1970s. Moreover, as noted earlier, Kim’s MSD guerrillas formed the core leadership of his regime which “was strong enough to shape the basic configuration of north Korean political culture.”<sup>95</sup> They were his followers but they were also his loyal comrades as well, and he trusted many of them to help him achieve his aims.

By 1961 Kim added 25 more of his guerrilla comrades to the KWP’s Central Committee (CC) and almost a decade later 13 more were added to the CC.<sup>96</sup> It seems plausible that as he consolidated power Kim empowered more of his guerrilla comrades to lead the core institutions of his regime. Suzy Kim appears to support this assertion. She argues that Kim Il-sung criticized the leaders of the local people’s committees (PCs) in 1952 for “coercively ordering the people around” like former colonial officials “rather than motivating them and working on their behalf as their ‘loyal servants’.” He reportedly advised that the leaders of the PCs should not “do all the work themselves, but rather to *delegate*,

engaging the participation of the majority of the people.” As North Korea was rebuilding itself after the Korean War, Kim encouraged them “to become self-reliant, ‘creatively deciding what to do in accordance with local conditions’ rather than ‘moving when pushed from the top, standing still without push, working like a machine by command, like puppets play’.” Suzy Kim implies that this kind of direct democracy based on the PCs began to change after 1972, as they merged with the cooperative farms.<sup>97</sup> Kim may have been willing to delegate because he was so confident that everything was going according to plan until the early 1970s.

The evidence suggests Kim was probably capable of exercising all four styles of leadership, to include some aspects of the delegating leadership style. In other words, after he purged his main opposition by the mid-1950s, he began to empower his trusted lieutenants and they helped him run the day-to-day operations of the affairs of state as they saw fit. To be sure, they were also subject to careful monitoring, and if they failed to meet Kim’s expectations they were likely to be purged (e.g., his guerrilla comrades who failed during the provocations of the late 1960s). Along with the members of the Kim family (e.g., his younger brother Kim Young-ju and later Kim Jong-il), many of Kim’s Manchurian guerrillas and select group of loyal elites such as Pang Hak-se from the Soviet faction served him well.<sup>98</sup> Others like the Kapsan group were not initially purged and appear to have been empowered, but when they challenged Kim’s authority over the succession issue in 1967 they too were purged. What does this mean for the role of brute power in Kim’s leadership style?

According to Burns, “The leadership approach tends often unconsciously to be elitist; it projects heroic figures against the shadowy background of drab, powerless masses.” His aim is to highlight both the leader and the follower and to judge the effectiveness of leaders “by actual social change measured by intent and satisfaction of human needs and expectations.” This means leadership goes beyond “mere power-holding” and is the antithesis of brute power. Subsequently, Burns identified transactional and transforming leadership as the two basic types of leadership. Transactional leadership is defined as “leaders approach[ing] followers with an eye to exchanging one thing for another: jobs for votes, or subsidies for campaign contributions.” On the other hand, transforming leadership is defined as identifying and exploiting “an existing need or demand of a potential follower” and creating a “relationship of mutual stimulation and elevation that converts followers into leaders and may convert leaders into moral agents.”<sup>99</sup> However, Watters pointed out that transformational leadership can be both positive and negative by noting that Adolf Hitler was a transformative leader, albeit a negative one.<sup>100</sup>

According to Chirot, Hitler as well as Mao and Stalin “were all thought to be exceptionally skillful at adapting to new circumstances, listening to other opinions within their parties, and learning from their experiences.”<sup>101</sup> Moreover, Burns credited Mao with being a “gifted political leader” because he understood what the masses needed and “the way in which those needs could be activated and channeled.” This allowed Mao to lead a transforming revolution in China that changed the very fabric of Chinese culture and society. This kind of revolutionary leadership can succeed when it has a “powerful value system,” can respond to the needs of the people, and can suppress dissent. However, Burns implied that, despite the need to suppress dissent, what men like Mao accomplished “qualifies as leadership when it [revolutionary leadership] is reciprocal in a situation of open conflict and as brute power when it is not.”<sup>102</sup> In other words, when revolutionary leaders believe only they possess the truth they become tyrants.<sup>103</sup> As a result, one could argue that the evidence suggests Kim Il-sung also led a transforming revolution in North Korea. Yet, when the regime promoted his cult of personality in the 1960s, his son instituted the monolithic guidance system in 1973, and the economy began to collapse near the end of his reign, Kim Il-sung eventually became more of a tyrant (albeit a popular one) and a negative transformational and transactional leader. This discussion of Kim’s leadership provides the basis for examining his successors’ leadership styles.

### THE RISE OF KIM JONG-IL AND THE ART OF TRANSFERRING CHARISMATIC LEADERSHIP

When Kim Jong-il became the successor, many “foreign analysts” believed he was “a playboy” and “would not outlive his father for too long, at least politically.”<sup>104</sup> They were all wrong. As noted earlier, Lankov acknowledged the younger Kim as a charismatic politician and shrewd manipulator who was just as skilled as his father.<sup>105</sup> The question is how did North Korea manage to transfer Kim Il-sung’s charismatic authority to his son? As discussed, Kim Il-sung’s legitimacy was based on his anti-Japanese guerrilla legacy and manipulated the patriarchal and charismatic authorities where the traditional social order, adoration of the people to the ruler, and the ruler’s “gifts of grace” reinforced his legitimacy. The evidence suggests Kim Jong-il eventually demonstrated his own charisma and benefited from Korea’s dynastic tradition.<sup>106</sup>

The North Koreans initially denounced Korea’s backward Confucian order but later restored it to prominence by emphasizing the two key tenets of *chung* (loyalty to the ruler or the state) and *hyo* (filial piety) to restore Korea’s

customary form of statecraft.<sup>107</sup> In this traditionally Korean (and East Asian)<sup>108</sup> context, Kim Il-sung’s authority as the *Suryong* is not simply derived from the people’s dependence on him but instead is a manifestation of his role as the sage father-ruler based on the “patriarchal, familial-political order.”<sup>109</sup> This narrative of Kim forming a lasting kinship with his guerrillas within the partisan family in Manchuria is constantly transmitted through epic stories, plays, films, poems, and art, and becomes the ideal familial relationship between the Kims and their people.<sup>110</sup> According to Lankov, while Kim Il-sung was “held in high esteem by many” North Koreans even after his death, “Kim Jong Il was probably the softest and most liberal” of the three Kims. In fact, he had reduced the number of political prisoners from about 200,000 in 1994 to no more than 90,000 by 2011. He also tolerated marketization from below, the growing border trade with China, and “chose not to punish excessively refugees found in China.”<sup>111</sup> Furthermore, as markets spread, North Koreans were increasingly being exposed to information that challenged the monopoly control of communication and altered their views about their own society. Hence, North Korea was losing its near-monopoly control of information and the people were much more aware of developments in the outside world.<sup>112</sup> In other words, Kim Jong-il may surprisingly have been a transformative leader by pragmatically tolerating these social changes in North Korea for a long time.

After Kim Il-sung’s death, his son derived his legitimacy in part “from his exemplary performance of his filial obligations to the nation’s dead father.”<sup>113</sup> He mourned his father’s death for three years like a good Confucian son of old, appointed his father as the country’s eternal President, inaugurated a new calendar to commemorate his birth, and built numerous monuments and a mausoleum to house his father’s embalmed body for all to see as if he were a living being.<sup>114</sup> With respect to charismatic authority, Kim Il-sung enjoyed one of its purest forms because of his anti-Japanese guerrilla legacy and, as we have seen above, he and his group of MSD guerrilla followers would form the core leadership of North Korea. In order to create the conditions for “hereditary charisma,” the North Koreans would have to completely manufacture Kim Jong-il’s ties to the guerrilla legacy.<sup>115</sup>

One of the important symbols concerning the transfer of power is the gift of a pistol from Kim Il-sung to his son. According to North Korean history, Kim Il-sung’s mother gave him the two pistols that his father left behind when Kim was 14 years old. The message his father conveyed was “armed struggle was the supreme form of struggle for national independence.”<sup>116</sup> In other words, those who took up arms to fight the Japanese would have the purest nationalist credentials. Upon receiving the pistols, Kim began to cultivate his own “unshakable revolutionary

resolve to restore national independence through armed struggle.” Moreover, North Koreans later claimed this was the true origin of Kim Jong-il’s military-first politics, the idea that many have attributed to him since his father’s death. This story, while likely manufactured, ties both Kims to the anti-Japanese and the anti-U.S. imperialist traditions of the North Korean revolution and reinforces the heroic nationalist bloodline of the Kim family.<sup>117</sup>

---

***Despite North Korea’s claims that the father was reluctant to choose his son as successor, the Supreme Leader probably had his own reasons for doing so despite Kim Jong-il’s lack of experience and accomplishments at the time.***

---

The problem that the Kims had to overcome was that “in the Communist movement, the positions of revolutionaries should be determined by the contributions they have made for the cause of the revolution and the people and by their future possibilities, and *should not be influenced in any way by blood relations.*”<sup>118</sup> According to Kim Jong-il’s hagiographers, the old Manchurian guerrillas were well aware of this revolutionary principle, but they nominated the younger Kim because they considered him the future of the Korean revolution. They claimed that Kim Il-sung remained uncharacteristically silent and indecisive during this discussion at the February 1974 plenary meeting of the KWP Political Committee. Kim’s guerrillas apparently sensed that he felt uneasy about his son becoming his successor and, although they had *always* carried out his orders unconditionally, this time “they would not obey the President’s intention.” Without any opposition from his guerrillas, Kim reportedly declared, “If all the committee members are in agreement, I have no objections to Kim Jong-il being elected to the Political Committee.”<sup>119</sup>

Despite North Korea’s claims that the father was reluctant to choose his son as successor, the Supreme Leader probably had his own reasons for doing so despite Kim Jong-il’s lack of experience and accomplishments at the time. According to Kim Young C., the Supreme Leader may have chosen his son for the following reasons:

First, the revolutionary cause of the great leader Kim Il Sung cannot be completed in a generation. It is a historic task that can be completed only through the efforts of succeeding generations. Second, the successor to the leader must emerge from the new generation, not from the present generation. *Third, it is necessary for a successor to the great leader to go through a preparatory period, learning and inheriting from the leader the thought,*

*theory, and art of leadership. Fourth, the successor should be a man who is boundlessly loyal to the leader and who embodies the leader’s ideology and leadership qualities* [emphasis added]. Jong Il, described as “endlessly loyal to the great leader, perfectly embodying the ideas, outstanding leadership, and noble traits of the leader, and brilliantly upholding the grand plan and intention of the leader at the highest level,” is said to provide the perfect answer to the question of succession.<sup>120</sup>

On the other hand, Lim argues that Kim Il-sung made the choice because of his concerns over the Soviets’ de-Stalinization campaign following the death of Stalin in 1953, Lin Biao’s attempted assassination of Mao after he became his successor, Kim Il-sung’s brother’s poor health, his guerrillas’ opposition to his second wife, and the state of his own health.<sup>121</sup> In other words, these factors led Kim to desire the most loyal successor who would promote his legacy while he was still alive.

Yet, Kim Jong-il had to demonstrate his leadership ability “in the art and literature sector” and impressed his father and his guerrillas when he successfully coordinated the Fifth Party Congress in 1970. He was also the oldest son of the Supreme Leader who had demonstrated capabilities to lead at a relatively young age.<sup>122</sup> This suggests performance also mattered, and challenges Weber’s suggestion that administrators in the charismatic leadership system are by and large selected based on their own charisma and personal loyalty to the ruler, *not* based on any special qualification. This suggests it is also plausible that the Kims may have chosen many of their senior administrators because of their capabilities to perform key tasks required for regime maintenance. In other words, the North Korean system’s success depends on the unity of the ruler and his administrative staff,<sup>123</sup> and his disciples’ ability to perform. As a result, it suggests Kim Jong-il was more than a transactional leader who used a directing style of leadership. Similar to his father, he probably derived his power from a mix of the ten sources of power that Watters discussed in his work, and Kim likely relied on both directing and coaching styles with personnel in key institutions. Despite U.S. Secretary of State Madeleine Albright’s impression that Kim’s subordinates “had little or no independence or flexibility,”<sup>124</sup> it is possible that like other effective leaders, based on the situation, he was capable of using supporting and even delegating styles<sup>125</sup> with those he trusted.

For example, as Kim Jong-il rose to power in the early 1970s, he commanded the Three Revolutions Movement of “young loyalists” to “weaken and sweep away the old guard,” and those who performed well “were fast-tracked to positions of power by Kim Jong Il.”<sup>126</sup> He trusted his negotiators, such as Kim Kye-kwan, and empowered him to negotiate on his



behalf. Moreover, when Kim reassigned General Kim Kyok-sik as the commander of the IV Corps prior to the provocations in 2010,<sup>127</sup> the Supreme Leader most likely delegated his authority to direct the operations near the Northern Limit Line (NLL). Finally, Kim Jong-il approved the appointment of Jang Song-thaek as a member of the National Defense Commission (NDC) in 2009 and Jang played a “crucial role” in promoting the leadership succession to his son.<sup>128</sup> Although one could argue Kim was a negative transformational leader because he failed to meet the needs and expectations of the majority of his people, Lankov emphasized that “it was Kim Il Sung’s policies that made disaster [of the 1990s] unavoidable.”<sup>129</sup> That being said, not many observers viewed the reclusive Kim Jong-il as a charismatic leader on the same level as his father. This perception began to change during the summer of 2000.

According to Lim Dong-un, former Director of South Korea’s National Intelligence Service (South Korea’s CIA equivalent) during the first North-South Summit between Kim Jong-il and former South Korean President Kim Dae-jung in June 2000, most observers simply assumed Kim Jong-il was “a strange dictator.” They also assumed Kim Jong-il had “succeeded to power despite his incompetency...while consistently practicing a tyranny of fear.” That is not all. Kim’s poor image also portrayed him as “impulsive and unpredictable” and “obstinate, militant, and cruel.”<sup>130</sup> However, after the summit, South Korean leaders described him as follows:

[The] Kim Jong-il we actually saw was a different person. He was well informed, intelligent, smart, and quick-witted; he had a vast accumulation of knowledge from his long, more than thirty-years of experience in important party positions. He was pleasant and had a good sense of humor. He showed *charisma and leadership* [emphasis added]... On the day of our arrival, the president and Chairman Kim had merely shook hands, but on the day of departure, they were now hugging each other... While observing the transformation in their relationship, I genuinely prayed that the North and South would also be close.<sup>131</sup>

The South Koreans were not the only ones who recognized Kim’s competence and leadership. A month after the Two Koreas Summit, Vladimir Putin became the first Russian (and former Soviet) leader to visit Pyongyang in July 2000. After the visit Putin described Kim as a “modern man” and praised both Kim’s ability to objectively observe world affairs and his flexibility.<sup>132</sup> This change in perspective of Kim Jong-il as a leader continued with the visit of former Secretary of State Madeleine Albright to Pyongyang in October 2000. After the visit she observed Kim Jong-il “was serious,” and confirmed other foreign leaders’ assessment that Kim “was

an intelligent man who knew what he wanted. He was isolated, not uninformed.”<sup>133</sup> The clear impression was Kim “made virtually all the decisions,” and as noted above Albright believed that “officials below him had little or no independence or flexibility.”<sup>134</sup>

---

***The South Koreans were not the only ones who recognized Kim’s competence and leadership. A month after the Two Koreas Summit, Vladimir Putin became the first Russian (and former Soviet) leader to visit Pyongyang in July 2000.***

---

The evidence, however, suggests Kim Jong-il relied on the core members of his regime to achieve his desired outcomes. Kim still used coercion after he consolidated power, but he seemed to have been judicious when he decided to do so. Kim, like his father, did not execute everyone for their failures.<sup>135</sup> Some were rehabilitated and Jang Song-thaek is a good example of this practice. He disappeared from public view in 2003 but returned in 2006 to play a powerful role in North Korea under Kim Jong-il.<sup>136</sup> In hindsight, Bruce Klingner observed in the fall of 2014, “Under Kim Jong-il, Pyongyang combined threats and assurances in a *comprehensive strategy*.” Kim had “raised brinksmanship to an art form in order to gain multiple policy goals” and, despite the hardline approach often associated with his rule, Pyongyang “always *calibrated* its position to avoid crossing the Rubicon.”<sup>137</sup>

In sum, once Kim Jong-il proved himself to be a worthy successor, the regime used a mix of neo-Confucian and familial (i.e., patriarchal) and charismatic (guerrilla and anti-imperialist legacy) legitimacy to restore Korea’s traditional style of statecraft and establish hereditary charismatic authority in North Korea. Once he consolidated power, Kim Jong-il’s leadership style was likely to have been a situational style that went beyond directing and transactional leadership. However, the use of other leadership styles (e.g., delegating) probably only applied to those within the true core elite or a select number of bureaucrats involved in key regime activities. Moreover, some even argued his rule may have been the “most liberal” by North Korean standards. As a result, the social change that he permitted continues to this day (i.e., positive transformational leadership), and he was eventually recognized for his intelligence, competence, flexibility, and strategic acumen. The evidence suggests Kim Jong-il’s rule led to a post-totalitarian transition in North Korea and he proved himself a charismatic leader. Next, the second North Korean leadership succession to Kim Jong-un will be examined.

## THE DEATH OF KIM JONG-IL AND REVIVAL OF KIM IL-SUNG'S CHARISMATIC LEADERSHIP



Figure 2. Photos of Kim Jong Un and his grandfather Kim Il-sung, <http://search.aol.com/aol/image?q=photo+of+kim+il+sung+and+kim+jong+un&v t=webmail-searchbox>.

Unlike his father, Kim Jong-un is “the spitting image of his grandfather when he came to power in the late 1940s, even to the point of shaving his sideburns up high” (see Figure 2). It is almost as if the regime was trying to make up for his lack of experience and leadership by arguing that “the DNA passed uncontaminated” from Kim Il-sung to his grandson.<sup>138</sup> The regime was carefully crafting his image to exploit Kim Il-sung’s cult of personality. According to a recent survey of defectors, this strategy appears to be working because “a significant number of North Koreans feel much hope about the third incarnation of Kimhood, finding the young leader attractive and somewhat charismatic.”<sup>139</sup> That being said, he still had to demonstrate his competence as a leader and did not wait too long to show he was developing those skills.

Kim Jong-un chose not to observe the normal 3-year mourning period when his father died, breaking from Confucian tradition that was observed after Kim Il-sung’s death. He only waited several months before he assumed power; some interpreted this as a message that Kim Jong-un would be different and gave hope that “the golden age of Kim Il Sung would return.”<sup>140</sup> Kim probably felt he had no choice but to show some early wins to demonstrate he was capable of becoming the Supreme Leader. He initially appeared to honor the nuclear deal with the U.S. that his father had approved in December 2011, but another space launch in April 2012 spoiled the deal.<sup>141</sup> It was soon apparent that the nuclear deal was not what Kim was looking for to demonstrate his leadership credentials. While his space launch raised tensions in April, Kim promised to improve the lives of his people.<sup>142</sup>

In May 2012, North Korea revised its constitution again and proclaimed, “In the face of the collapse of the world socialist system and the vicious offensive of the imperialist allied forces to stifle the Democratic People’s Republic of Korea, Comrade Kim Jong-il administered *Songun* politics; thus he safeguarded with honour the achievements of socialism which are the precious legacy of Comrade Kim Il-sung.” Kim Jong-il was also credited with developing North Korea as “a nuclear state and an unchallengeable military power.” Kim Jong-il was thus granted the title of “Eternal Chairman” of the NDC and Kim Jong-un was given the new title “First Chairman” of the NDC.”<sup>143</sup> What this indicated was that to bolster his lack of legitimacy Kim Jong-un would justify his policies by recalling the existing policies and accomplishments of his forefathers.

---

*Kim Jong-un chose not to observe the normal 3-year mourning period when his father died, breaking from Confucian tradition that was observed after Kim Il-sung’s death.*

---

The U.S. and others in the international community issued another United Nations Security Council (UNSC) resolution to “censure” North Korea after the December 2012 space launch. The resolution targeted key personnel involved in Pyongyang’s nuclear and missile programs and levied international pressure to deter further testing of its missiles. North Korea responded to the sanctions by conducting a third nuclear test on February 13, 2013. After the test, it claimed it had “miniaturized” a nuclear device in “a safe and perfect manner.”<sup>144</sup> The problem for the U.S. is that the provocations did not end with the reported miniaturization test as the military began to prepare for its annual training exercise with the South Koreans. On March 7, 2013, North Korea condemned the combined U.S.-South Korea Exercise FOAL EAGLE that was being conducted from March 1 to April 30. A Korea Central News Agency (KCNA) commentary highlighted that many U.S. “ultra-modern nuclear war means,” such as a nuclear aircraft carrier, B-52 bombers, and F-22 stealth fighters, were going to be involved in the exercises. The KCNA took issue with South Korean claims that “B-52 and F-22 are ‘capable of preempting an attack on the abode of the headquarters of the north’ being undetected by radar.” It concluded, “This proves that the on-going drills are an unpardonable terrorist act and a drill for preemptive nuclear attack aimed at harming the headquarters of the revolution and the social system in the DPRK.”<sup>145</sup>

The Central Committee of the KWP adopted a new strategic line on March 31, 2013, aimed to expand the regime's nuclear capabilities as well as its economic development (i.e., *Byungjin* line).<sup>146</sup> Perhaps more importantly, the regime also revealed that the *Byungjin* line was initiated by Kim Il-sung in 1962. This inexorably legitimized the policy and signaled Kim Jong-un would attempt to honor his grandfather by building a "powerful socialist nation."<sup>147</sup> The North Koreans continued to characterize the combined exercise in South Korea as the "largest-ever nuclear war maneuvers" preparing to topple the regime. Pyongyang followed this up by nullifying the Korean Armistice Agreement as well as all existing North-South agreements of non-aggression.<sup>148</sup> The Supreme Command placed the entire country on war footing on March 11, 2013,<sup>149</sup> and Kim visited a KPA unit near the DMZ to demonstrate his leadership.<sup>150</sup> The stage was set for Kim to show his ability to defend the sovereignty of North Korea against the U.S. imperialists.

---

*On May 13, 2013, Pyongyang announced that it would never give up its eternal treasure of the nation—its nuclear weapons.*

---

The Supreme People's Assembly (SPA) passed a law on April 1, 2013, stating that North Korea "is a full-fledged nuclear weapons state." It claimed its nuclear weapons were a "just means for defence" and served "the purpose of deterring and repelling the aggression and attack of the enemy against the DPRK and dealing deadly retaliatory blows at the strongholds of aggression until the world is denuclearized."<sup>151</sup> Kim Jong-un subsequently visited several military units and deployed his missile units to the eastern coast. Some observers speculated the deployed missiles were targeting Guam.<sup>152</sup> On April 4, Seoul "confirmed that Pyongyang has moved a missile with 'considerable range' to its east coast." This confirmation from Seoul came after the KPA had announced it had been "authorised to attack the US using 'smaller, lighter and diversified' nuclear weapons." Some in Japan began to speculate "the missile could be a KN-08, which is believed to be a long-range [mobile] missile that—if operable—could hit the US."<sup>153</sup> Others in the U.S. had disclosed that DIA "assessed with 'moderate confidence' that North Korea has the ability to deliver a nuclear weapon with a ballistic missile, though the reliability is believed to be 'low'."<sup>154</sup> On May 13, 2013, Pyongyang announced that it would never give up its eternal treasure of the nation—its nuclear weapons. It stated, "There have been big and small wars in the world for nearly seven decades since the appearance of nuclear weapons but nuclear weapons states have never been exposed to any war."<sup>155</sup>

Under Kim Jong-un, North Korea claimed it possessed "smaller, lighter and diversified powerful nuclear deterrence." As a result, the U.S. could no longer threaten it with nuclear weapons, and Pyongyang's "nukes can never be a bargaining chip under any circumstances as they are stipulated by a law of the DPRK."<sup>156</sup> In the end, the missile deployment to the east coast was only a demonstration of force, but it appeared to make the point that Kim is capable of defending the North's sovereignty and he is serious about reviving his grandfather's *Byungjin* policy. That is not all; in October 2015, he manufactured another crisis to take advantage of the 70<sup>th</sup> anniversary of Korea's liberation from Japanese colonial rule. It was intended to spotlight the North's revolutionary credentials by discrediting Japanese colonialism, former South Korean President Park Chung-hee's colonial legacy (see Figure 3), and his daughter's administration in Seoul, and to argue for a self-reliant path toward reunification.

### **PYONGYANG DRAWS SPOTLIGHT TO TOUT ITS ANTI-JAPANESE LEGACY**

**K**im Jong-un most likely manufactured a landmine incident in August 2015 to legitimize his role as the Supreme Leader. He attempted to do so by spotlighting both Koreas' colonial legacy with Japan. The day the incident occurred, KCNA mentioned a South Korean newspaper's claim of a "sordid nexus between traitor Park Chung-hee, father of the present puppet chief executive of south Korea [Park Geun-hye], and the Mitsubishi Group of Japan." It went on to claim that after Park's military coup he received one million U.S. dollars from Mitsubishi as a "political fund" during the presidential election of 1963. The North Koreans accused Park of giving Mitsubishi near-monopoly control of South Korea's economy, which made Seoul a "dependent sub-contract industry and a processing base" for the Japanese firm. Park was a "pro-Japanese lackey" that joined hands with a Japanese firm which actively supported Japan during World War II and inflicted "untold pain and damage upon Koreans."<sup>157</sup> The North also accused Park of taking huge sums of money from Japanese firms during the 1971 presidential election, and accused his daughter of being a "wicked traitor as her father." Pyongyang took issue with Park Geun-hye considering normalization of relations with Japan while Tokyo refuses to issue "an apology and reparation for its past crimes."<sup>158</sup>





**Figure 3.** Former South Korean President Park Chung-hee as a Japanese Army Lieutenant, <http://www.sakai.zaq.ne.jp/duelv307/img721.jpg>.

This was unacceptable to all Koreans from the North's perspective since Japanese Prime Minister Shinzo Abe was "so arrogant as to bluster that the issue of comfort women can be settled by paying about three hundred million yen... Mitsubishi [also] refused to make reparation for the loss suffered by Koreans who had been forced to do slave labor during the Japanese imperialists' colonial rule over Korea."<sup>159</sup> What seemed to be most offensive to Pyongyang was the fact that Park Geun-hye was sharing intelligence about North Korea with Japan "at the instigation of the U.S." It stated Park's "sycophancy toward Japan is, indeed, the most humiliating act of sycophancy and hideous act of treachery putting into the shade not only traitor Park Chung-hee but also the five traitors of 1905 [who signed away Korea's sovereignty to Japan]." Pyongyang called for investigation of both of their crimes and stated they "should be sternly punished by the nation for kissing Japan, the sworn enemy."<sup>160</sup> In short, North Korea was reminding all Koreans it was more legitimate than the Park regime as the 70<sup>th</sup> anniversary of Korea's liberation from Japanese colonial rule was looming on August 15.

Against this background, the landmine incident brought the spotlight back on North Korea. On August 6, Pyongyang announced that it would turn back the clock 30 minutes to reclaim its sovereignty from yet another vestige of Japanese imperialism. Many observers simply discounted the time zone change as more "bizarre"<sup>161</sup> behavior by the rogue regime in Pyongyang. However, the regime justified the time change by declaring, "The wicked Japanese imperialists committed such unpardonable crimes as depriving Korea of even its standard time while mercilessly trampling down its land with 5000 year-long history and culture and pursuing the unheard-of policy of obliterating the Korean nation."<sup>162</sup>

On August 16, a spokesman for the Committee for the Peaceful Reunification of Korea continued to attack President Park in the South for staging nuclear war exercises, anti-regime leaflet operations, human rights allegations, and "other rows against the DPRK." It accused her of dampening "the aspiration of all Koreans and their efforts to make August 15 an important occasion of north-south reconciliation and national unity by conducting anti-north psychological broadcasting and leaflet scattering operations in the wake of the fabrication of the 'mine explosion,' a poor farce."<sup>163</sup>

The KPA responded by firing rockets across the DMZ on August 20 and the South Korean Army quickly returned counter-artillery fires into North Korea. The U.S. urged Pyongyang to cease its provocations as tensions quickly escalated on the peninsula. North Korea chose not to return fire<sup>164</sup> and the next day denied responsibility for the landmine incident, accusing the "south Korean puppet military gangsters" of manufacturing the "doubtful" landmine incident in the DMZ to justify the resumption of its "anti-DPRK psychological warfare." It called the loudspeaker and "leaflet-scattering" operations an act of war and announced that the General Staff of the KPA issued an ultimatum to the South Korean military that, unless it ceased the anti-regime loudspeaker broadcasts and "removes all psywar [psychological warfare] means within 48 hours," Seoul would face "strong military action." KCNA disclosed that Kim Jong-un had called an emergency "enlarged" meeting of the KWP's Central Military Commission (CMC) during the evening of August 20, which included senior leaders of the KPA General Staff, frontline commanders, senior officials of the intelligence and security services, leading officials of the KWP, and "officials in charge of external affairs." Most importantly, it was revealed Kim had "issued an order of the supreme commander of the Korean People's Army that the frontline large combined units of the KPA should enter a wartime state to be fully battle ready to launch surprise operations and the area along the front be put in a semi-war state."<sup>165</sup>



South Korea responded by ordering its own troops to prepare for war on August 21, 2015.<sup>166</sup> The U.S. and South Korea also briefly halted Exercise ULCHI FREEDOM GUARDIAN (UFG) to coordinate a measured but strong response to North Korean provocations and hinted U.S. strategic assets would be deployed to Korea again.<sup>167</sup> The situation began to escalate as Seoul “vowed to hit back with overwhelming strength” in case of further North Korean attacks against South Korea.<sup>168</sup> Just as the crisis appeared to escalate out of control, the North Koreans proposed high-level talks. The two sides met August 22-24 at Panmunjom and, after Pyongyang finally expressed “regret” for the landmine attack on August 24, Seoul agreed to shut down the loudspeaker operations along the DMZ. Both sides also agreed to resume family reunions and continue discussions to resolve other differences. The U.S. State Department welcomed the agreement and hoped “it leads to decreasing tensions on the peninsula.”<sup>169</sup>

---

***...during his “reign of terror” Kim has executed about 70 high-level officials since assuming power in December 2011, to include his uncle Jang Song-thaek.***

---

After the landmine incident, several North Korea observers acknowledged Kim had demonstrated his competence by performing better during this crisis than anticipated. According to David Garretson, a retired professor from the University of Maryland branch in Seoul, Kim “has finally got a feel for things,” and his “experience of juggling many balls has matured him.” He also demonstrated that he was “more rational” and seemed to have “good command and control” of the situation. Kim Jung-bong, a former South Korean official, agreed by stating, “Kim Jong Un is much more calculating and careful than we knew... We have to take him seriously.” According to another professor from a Korean university in Seoul, Yoo Chan-yul, Seoul’s “decisiveness and refusal to back down on the propaganda broadcasts” led Kim to seek a face-saving way out. However, Kim “showed political savvy” by “backing down.” Yoo concluded, “He’s a real tough cookie, more than we realized... He may be tyrannical and vicious, but maybe Kim Jong Un is realistic as well.”<sup>170</sup>

According to John Grisafi, during his “reign of terror” Kim has executed about 70 high-level officials since assuming power in December 2011, to include his uncle Jang Song-thaek.<sup>171</sup> As we have seen, these purges follow the long-established tradition of his grandfather who also purged all of his rivals during the early phase of his power consolidation. However, once he became the Supreme Leader, Kim Il-sung relied on milder forms of punishment to

maintain control. Having said that, the following highlights how Kim Jong-un is likely following Kim Il-sung’s lead to control his core elites and indicates why he may have already consolidated his power.<sup>172</sup>

In recent months, there have been numerous cases of North Korean elites reemerging after months of absence from public view. For several of these officials, there is evidence to suggest they were undergoing re-education and even punishment due to some infraction or shortcoming. These examples may be evidence of a shift in Kim Jong Un’s method of disciplining senior officials and exerting his supreme authority over regime elites. This trend itself may be a sign that Kim and the rest of the core leadership now feel more secure and stable as the rulers of North Korea.<sup>173</sup>

It is also important to note that Kim Jong-un has also overlooked the spread of markets and is aware that more of his people are being exposed to information which contradicts the regime’s propaganda. He may have decided it is futile to consider regaining complete control of markets and information. For example, when the regime attempted to regain “political control” through currency reform in 2009, it failed. Subsequently, North Korea’s Premier Kim Yong-il stated, “I sincerely apologize as we pushed ahead with it without a sufficient preparation so it caused a big pain to the people” and the state “will do its best to stabilize people’s lives”.<sup>174</sup> This indicated North Korea had transitioned to a post-totalitarian state near the end of Kim Jong-il’s regime. Hence, what is more important for Kim Jong-un is to deliver results—he must show he can achieve *Byungjin*.

---

***In 2016 North Korea conducted its fourth nuclear test and launched several missiles capable of delivering nuclear weapons. Kim has also invested heavily in the economy and conventional weapons, which suggests Byungjin remains a priority of the regime.***

---

In 2016 North Korea conducted its fourth nuclear test<sup>175</sup> and launched several missiles capable of delivering nuclear weapons. Kim has also invested heavily in the economy and conventional weapons, which suggests *Byungjin* remains a priority of the regime.<sup>176</sup> What is more significant is that these efforts have been accompanied by “noticeable personnel changes that emphasize competence over political flunkeyism.” While it is a stretch to call this a move toward meritocracy, “there is a push towards more competent people.” Moreover, these achievements could not have been accomplished without economic growth. Curtis Melvin

argues that North Korea could not have pursued these initiatives simultaneously with only one or two percent growth. Melvin argues, “There’s been a massive increase in public spending on both the economic side—like factories and entertainment facilities—and on the military side.”<sup>177</sup> During the 7<sup>th</sup> Workers’ Party Congress in May 2016, it was clear the concept of the *Suryong* and the “‘Theory of the Revolutionary Family’ based on *Juche* are the core ideological foundations providing political legitimacy to the inheritance of power throughout the three generations of Kims.”<sup>178</sup> Thus far, Kim appears to have demonstrated that his revival of *Byungjin* policy is more than an aspirational goal and he is willing to use any means to consolidate his power. However, he still relies on the legacies of the first two Kims to demonstrate his competence and charismatic leadership. If he is to survive, he must rely on competent civilian and military leaders to implement his domestic and external strategies and achieve his aims.

---

*The Western media often promote the perception that North Korean leaders are “bizarre, irrational, demonic, and self-destructive.” However, evidence suggests the first two Kims were capable and charismatic leaders, and Kim Jong-un is following their lead to demonstrate his competence and potential as the Supreme Leader.*

---

## CONCLUSION

The Western media often promote the perception that North Korean leaders are “bizarre, irrational, demonic, and self-destructive.” However, evidence suggests the first two Kims were capable and charismatic leaders, and Kim Jong-un is following their lead to demonstrate his competence and potential as the Supreme Leader. In the end, this study reveals North Korea’s grand strategy. Nye defined it as the country’s “leaders’ theory and story about how to provide for its security, welfare, and identity,” but in order for the grand strategy to work it “has to be adjusted for changes in context.”<sup>179</sup> Hence, one could argue North Korea’s grand strategy is founded on its anti-imperialist legacy, *Juche* ideology, and the possession of nuclear weapons. Kim Jong-il adjusted for the changes that occurred after his father’s death by promoting his military-first politics but contributed to North Korea’s grand strategy by finally producing nuclear weapons. It appears that Kim Jong-un’s contribution will be to enhance the nuclear deterrent by acquiring nuclear ICBMs, and his policy adjustment is to embrace his grandfather’s *Byungjin* policy to improve the economy.

Kim Jong-un probably knows he cannot become the undisputed Supreme Leader if the only thing going for him is the pure blood inherited from his grandfather or terroristic police control. As discussed, there are indications that, after purging about 70 of his core elites, Kim may be easing up on his purges to build unity among the core leadership. This suggests he is more confident about having consolidated his power. After eliminating immediate threats to his rule, he may be varying his leadership style to coopt the regime’s core elites. Moreover, Kim must be able to deliver economic success to provide a better life for his people so they are willing to support his regime’s policies as North Korea continues its post-totalitarian transition. In case of failure, Kim could try to find a scapegoat but a better informed populace may not be willing to go on another arduous march if the famine returns. As a result, despite Pyongyang’s demonstrated resilience, Kim has significant challenges ahead at home and abroad. He will have to cultivate his leadership skills to survive but he seems to be doing better than anticipated, and after surviving the first five years of his rule time may be on his side.

## NOTES

<sup>1</sup> Jasper Becker, *Rogue Regime: Kim Jong Il and The Looming Threat of North Korea* (Oxford, UK: Oxford University Press, 2005), p. ix.

<sup>2</sup> Becker, *Rogue Regime*, p. xiv.

<sup>3</sup> Peter G. Northouse, *Leadership: Theory and Practice*, 7th ed. (Thousand Oaks, CA: Sage Publications, Inc., 2016), pp. 12-13.

<sup>4</sup> Joseph S. Nye, Jr., *The Powers to Lead* (Oxford, UK: Oxford University Press, 2008), pp. 38-39.

<sup>5</sup> Helen-Louise Hunter, *Kim Il-song’s North Korea* (Westport, CT: Praeger, 1999), pp. 22-25.

<sup>6</sup> Jane Portal, *Art Under Control in North Korea* (London, UK: Reaktion Books, Ltd., 2005), p. 99.

<sup>7</sup> Portal, *Art Under Control in North Korea*, p. 98.

<sup>8</sup> Paul French, *North Korea: State of Paranoia* (New York: Zed Books, 2014), p. 398.

<sup>9</sup> Samuel S. Kim, *The North Korean System in the Post-Cold War Era* (New York: Palgrave, 2001), p. 13.

<sup>10</sup> Bruce Cumings, “The Kims’ Three Bodies: Communism and Dynastic Succession in North Korea,” *Current History*, September 2012,” p. 218.

<sup>11</sup> Andrei Lankov, *The Real North Korea: Life and Politics in the Failed Stalinist Utopia* (Oxford, UK: Oxford University Press, 2013), p. 69.

<sup>12</sup> Michael E. Robinson, *Korea’s Twentieth-Century Odyssey: A Short History* (Honolulu: University of Hawaii Press, 2007), p. 147.

<sup>13</sup> Charles Armstrong, *The North Korean Revolution: 1945-1950* (Ithaca, NY: Cornell University Press, 2003), p. 55.

<sup>14</sup> Carl J. Friedrich and Zbigniew K. Brzezinski, *Totalitarian Dictatorship and Autocracy* (New York: Frederick A. Praeger Publisher, 1964), pp. 9-10.

<sup>15</sup> Cheong, Sung-Hwa, *The Politics of Anti-Japanese Sentiment in Korea: Japanese-South Korean Relations Under American Occupation, 1945-1952* (New York: Greenwood Press, 1991), pp. xi-xiv.

- <sup>16</sup> Kim Jongwon, *Divided Korea: The Politics of Development, 1945-1972* (Elizabeth, NJ: Hollym, 1997), pp. 39-40.
- <sup>17</sup> Kim Il Sung, *With the Century*, Volume 2 (Pyongyang, Korea: Foreign Languages Publishing House, 1992), pp. 68-69.
- <sup>18</sup> Han Hong-koo, "Wounded Nationalism: The Minsaengdan Incident and Kim Il Sung in Eastern Manchuria" (PhD diss., University of Washington, 1999), pp. 76-77.
- <sup>19</sup> Han, "Wounded Nationalism," pp. 179-180.
- <sup>20</sup> Han, "Wounded Nationalism," p. 334. According to Han, a group of pro-Japanese Koreans in Kando (Chientao in Chinese) established the MSD – People's Livelihood Corps – in February 1932. The MSD declared "its aim was to secure the livelihood of 400,000 Koreans in Kando and to build an earthly paradise for Koreans." The MSD promoted Korean autonomy in Kando; some of its members even said Kando had historically been part of Korea and they had legitimate claims to the land. The Chinese turned against them after rumors spread of pro-Japanese MSD agents.
- <sup>21</sup> Armstrong, *The North Korean Revolution*, p. 55.
- <sup>22</sup> Andrei Lankov, *From Stalin to Kim Il Sung: The Formation of North Korea 1945-1960* (New Brunswick, NJ: Rutgers University Press, 2002), pp. 8-9.
- <sup>23</sup> Bruce Cumings, *Korea's Place in the Sun: A Modern History* (New York: W.W. Norton & Company, 1997), pp. 230-232.
- <sup>24</sup> Suh Dae-Sook and Lee Chae-Jin, eds., *Political Leadership in Korea* (Seattle, WA: University of Washington Press, 1976), p. 164.
- <sup>25</sup> Nam Koon Woo, *The North Korean Communist Leadership, 1945-1965* (Tuscaloosa: The University of Alabama Press, 1974), pp. 110-115.
- <sup>26</sup> Nam, *The North Korean Communist Leadership*, pp. 110-115.
- <sup>27</sup> Suh and Lee, eds., *Political Leadership in Korea*, p. 164.
- <sup>28</sup> According to Lim Jae-cheon, the Kapsan faction should not be considered as Kim Il-sung's faction. While it is true that this group formed an underground network in Kapsan to fight the Japanese and made contacts with Kim's guerrillas starting in 1936, they should be considered as a separate domestic Communist group.
- <sup>29</sup> Lim Jae-cheon, *Kim Jong Il's Leadership of North Korea* (New York: Routledge, 2009), pp. 39-40.
- <sup>30</sup> Kim Il Sung, *With the Century*, Volume 7 (Pyongyang, Korea: Foreign Languages Publishing House, 2007), pp. 136-149.
- <sup>31</sup> Cumings, *Korea's Place in the Sun*, pp. 230-232.
- <sup>32</sup> Bernd Schaefer, "North Korean 'Adventurism' and China's Long Shadow, 1966-1972," North Korea International Documentation Project, Working Paper #44, Woodrow Wilson International Center for Scholars, October 2004, pp. 3-11.
- <sup>33</sup> Portal, *Art Under Control in North Korea*, pp. 98-99.
- <sup>34</sup> Robinson, *Korea's Twentieth-Century Odyssey*, p. 159.
- <sup>35</sup> Bernd Schaefer, "North Korean 'Adventurism' and China's Long Shadow, 1966-1972," North Korea International Documentation Project, Working Paper #44, Woodrow Wilson International Center for Scholars, October 2004, pp. 3-11.
- <sup>36</sup> Ken Gause, "Coercion, Control, Surveillance, and Punishment," The Committee for Human Rights in North Korea, 2012, pp. 92-95.
- <sup>37</sup> Joseph S. Bermudez, Jr., *The Armed Forces of North Korea* (London: I.B. Tauris Publishers, 2001), p. 1.
- <sup>38</sup> Hunter, *Kim Il-song's North Korea*, pp. 25-26.
- <sup>39</sup> Han, "Wounded Nationalism," p. 358.
- <sup>40</sup> Paul Fischer, *A Kim Jong-il Production: The Extraordinary True Story of a Kidnapped Filmmaker, His Start Actress, and a Young Dictator's Rise to Power* (New York: Flatiron Books, 2015), pp. 308-310.
- <sup>41</sup> Kim Suk-Young, *Illusive Utopia: Theater, Film, and Everyday Performance in North Korea* (Ann Arbor: University of Michigan Press, 2010), pp. 33-59.
- <sup>42</sup> Kim, *Illusive Utopia*, pp. 33-59.
- <sup>43</sup> Lee Chong-sik, *Korean Workers' Party: A Short History* (Stanford, CA: Hoover Institution Press, 1978), p. 133.
- <sup>44</sup> Cumings, *Korea's Place in the Sun*, pp. 402-404.
- <sup>45</sup> Cumings, "The Kims' Three Bodies," p. 218.
- <sup>46</sup> Charles K. Armstrong, "'Fraternal Socialism': The International Reconstruction of North Korea, 1953-62," *Cold War History*, Vol. 5, No. 2, May 2005, p. 165. According to Armstrong, the East Germans had been supporting the North Koreans since September 1950 (e.g., provided 11.6 million Deutsche Marks worth of supplies, to include about 150,000 kilograms of medicine and two ambulances).
- <sup>47</sup> Erik Cornell, *North Korea Under Communism: Report of an Envoy to Paradise* (New York: RoutledgeCurzon, 2002), p. 66.
- <sup>48</sup> Charles K. Armstrong, "Juche and North Korea's Global Aspirations," North Korea International Documentation Project, Working Paper #1, Woodrow Wilson International Center for Scholars, April 2009, pp. 1-8.
- <sup>49</sup> Cornell, *North Korea Under Communism*, p. 72.
- <sup>50</sup> John G. Grisafi, "Kim Jong Un may be easing reign of terror over elites: Shift from purge by execution to punishment by reeducation possible sign of stabilizing regime," November 30, 2015, <https://www.nknews.org/2015/11/kim-jong-un-may-be-easing-reign-of-terror-over-elites/> (accessed December 11, 2015).
- <sup>51</sup> James Macgregor Burns, *Leadership* (New York: HarperCollins Publishers, 1978), pp. 3-4.
- <sup>52</sup> Tim Beal, *North Korea: The Struggle Against American Power* (London: Pluto Press, 2005), p. 38.
- <sup>53</sup> Lim Um, *The Founding of a Dynasty in North Korea: An Authentic Biography of Kim Il-song* (Tokyo: Jiyu-sha, 1982), pp. 2-52.
- <sup>54</sup> Han, "Wounded Nationalism," pp. 16-17.
- <sup>55</sup> Han, "Wounded Nationalism," p. 76.
- <sup>56</sup> Han, "Wounded Nationalism," pp. 179-180.
- <sup>57</sup> Kim Il Sung, *With the Century*, Volume 4 (Pyongyang, Korea: Foreign Languages Publishing House, 1993), pp. 39-40.
- <sup>58</sup> Han, "Wounded Nationalism," pp. 76-77.
- <sup>59</sup> Han, "Wounded Nationalism," pp. 186-188.
- <sup>60</sup> Han, "Wounded Nationalism," pp. 178-179.
- <sup>61</sup> Han, "Wounded Nationalism," pp. 186-188.
- <sup>62</sup> Han, "Wounded Nationalism," pp. 93-98.
- <sup>63</sup> Han, "Wounded Nationalism," pp. 98-99.
- <sup>64</sup> Armstrong, *The North Korean Revolution*, p. 28.
- <sup>65</sup> Kim Il Sung, *With the Century*, Volume 2, pp. 68-69.
- <sup>66</sup> Han, "Wounded Nationalism," p. 10.
- <sup>67</sup> Han, "Wounded Nationalism," p. 354.
- <sup>68</sup> Han, "Wounded Nationalism," p. 19.
- <sup>69</sup> Han, "Wounded Nationalism," pp. 331-337 and pp. 341-346.
- <sup>70</sup> Han, "Wounded Nationalism," pp. 331-337 and pp. 353-354.
- <sup>71</sup> Han, "Wounded Nationalism," pp. 322-323.
- <sup>72</sup> Han, "Wounded Nationalism," pp. 329-330.
- <sup>73</sup> Baik Bong, *Kim Il Sung: Biography*, Volume [I] (Beirut, Lebanon: Dar Al-Talia, 1973), pp. 346-347.
- <sup>74</sup> Han, "Wounded Nationalism," p. 334.



- <sup>75</sup> Han, "Wounded Nationalism," pp. 329-334.
- <sup>76</sup> Han, "Wounded Nationalism," p. 354.
- <sup>77</sup> John Tirman, *The Deaths of Others: The Fate of Civilians in America's Wars* (Oxford, UK: Oxford University Press, 2011), p. 93.
- <sup>78</sup> Robert Cooper, *The Breaking of Nations: Order and Chaos in the Twenty-First Century* (New York: Atlantic Monthly, 2003), p. 88.
- <sup>79</sup> Max Weber, "The Three Types of Legitimate Rule," *Berkeley Publications in Society and Institutions*, Vol. 4, No. 1, 1958, p. 1.
- <sup>80</sup> Weber, "The Three Types of Legitimate Rule," p. 2.
- <sup>81</sup> Daren C. Zook, "Reforming North Korea: Law, Politics, and the Market Economy," *Stanford Journal of International Law*, Vol. 48, No. 1, 2012, pp. 134-139.
- <sup>82</sup> Zook, "Reforming North Korea," pp. 3-4.
- <sup>83</sup> Juan J. Linz and Alfred Stepan, *Problems of Democratic Transition and Consolidation: Southern Europe, South America, and Post-Communist Europe* (Baltimore, MD: Johns Hopkins University Press, 1996), p. 51.
- <sup>84</sup> Linz and Stepan, *Problems of Democratic Transition and Consolidation*, p. 53.
- <sup>85</sup> Max Weber, "The Three Types of Legitimate Rule," pp. 6-8.
- <sup>86</sup> Max Weber, "The Three Types of Legitimate Rule," pp. 6-8.
- <sup>87</sup> Joseph S. Nye, Jr., *The Future of Power* (New York: Public Affairs, 2011), p. 10. Nye offers other definitions of power such as "the ability to get what we want," "the ability to make or resist change," or "the capacity to do things and in social situations to affect others to get the outcomes we want." For the latter, Nye laments that some equate it with influence which confuses the discussion about power.
- <sup>88</sup> Gina Abudi, "The Five Types of Power in Leadership," Intuit QuickBase, <http://quickbase.intuit.com/blog/2011/08/26/the-5-types-of-power-in-leadership/> (accessed August 6, 2015). Abudi's discussion of the bases of power breaks them down into two parts: formal and personal power. Formal power is derived from the combination of coercive, reward and legitimate powers, and personal power results from expert and referent powers.
- <sup>89</sup> Vivian Giang, "The 7 Types of Power that Shape the Workplace," <http://www.businessinsider.com/the-7-types-of-power-that-shape-the-workplace-2013-7> (accessed August 7, 2015). Giang also introduces the concept of connection power, which she described as "where a person attains influence by gaining favor or simply acquaintance with a powerful person. This power is all about networking."
- <sup>90</sup> Bryan Shaun Charles Watters, "Contemporary British Military Leadership in the Early Twenty First Century," (PhD diss., University of Leeds Business School, February 2008), pp. 44-46.
- <sup>91</sup> Daniel Chirot, *Modern Tyrants: The Power and Prevalence of Evil in Our Age* (New York: The Free Press, 1994), pp. 247-248.
- <sup>92</sup> Northouse, *Leadership*, 7th ed., p. 93.
- <sup>93</sup> Peter G. Northouse, *Leadership: Theory and Practice*, 6th ed. (Thousand Oaks, CA: Sage Publications, Inc., 2013), pp. 101-102.
- <sup>94</sup> Lim, *Kim Jong Il's Leadership of North Korea*, p. 68.
- <sup>95</sup> Han, "Wounded Nationalism," pp. 331-337 and pp. 353-354.
- <sup>96</sup> Suh and Lee, eds., *Political Leadership in Korea*, p. 164.
- <sup>97</sup> Suzy Kim, *Everyday Life in the North Korean Revolution, 1945-1950* (Ithaca, NY: Cornell University Press, 2013), pp. 247-248.
- <sup>98</sup> Gause, "Coercion, Control, Surveillance, and Punishment," pp. 92-95.
- <sup>99</sup> Burns, *Leadership*, pp. 3-4.
- <sup>100</sup> Watters, "Contemporary British Military Leadership in the Early Twenty First Century," p. 59.
- <sup>101</sup> Chirot, *Modern Tyrants*, p. 421.
- <sup>102</sup> Burns, *Leadership*, pp. 235-239.
- <sup>103</sup> Chirot, *Modern Tyrants*, p. 421.
- <sup>104</sup> Lankov, *The Real North Korea*, p. 69.
- <sup>105</sup> Lankov, *The Real North Korea*, p. 69.
- <sup>106</sup> Daren C. Zook, "Reforming North Korea: Law, Politics, and the Market Economy," p. 139.
- <sup>107</sup> Kwon, Heonik, and Chung Byung-Ho, *North Korea: Beyond Charismatic Politics* (Lanham, MD: Rowman & Littlefield Publishers, Inc., 2012), p. 19.
- <sup>108</sup> Anne Prescott, *East Asia in the World: An Introduction* (New York: Routledge, 2015), pp. 174-181.
- <sup>109</sup> Kwon and Chung, *North Korea: Beyond Charismatic Politics*, p. 26.
- <sup>110</sup> Kwon and Chung, *North Korea: Beyond Charismatic Politics*, pp. 26-66.
- <sup>111</sup> Andrei Lankov, "Kim Jong Un's popularity, explained," NK News.Org, September 27, 2015, <http://www.nknews.org/2015/09/kim-jong-uns-popularity-explain/> (accessed September 27, 2015).
- <sup>112</sup> Nat Kretchun and Jane Kim, "A Quiet Opening: North Koreans in a Changing Media Environment," *InterMedia* (Washington, DC: InterMedia, May 2012), p. 1.
- <sup>113</sup> Kwon and Chung, *North Korea: Beyond Charismatic Politics*, pp. 14-66.
- <sup>114</sup> Kwon and Chung, *North Korea: Beyond Charismatic Politics*, pp. 71-75.
- <sup>115</sup> Kwon and Chung, *North Korea: Beyond Charismatic Politics*, pp. 83-89.
- <sup>116</sup> Kwon and Chung, *North Korea: Beyond Charismatic Politics*, p. 83.
- <sup>117</sup> Kwon and Chung, *North Korea: Beyond Charismatic Politics*, pp. 83-89.
- <sup>118</sup> Tak Jin, Kim Gang-il, and Pak Hong-je, *Great Leader: Kim Jong Il*, Volume [II] (Tokyo: Sorinsha Publishers, 1986), p. 16.
- <sup>119</sup> Tak, Kim, and Pak, *Great Leader*, pp. 15-17.
- <sup>120</sup> Kim, Young C., "North Korea in 1980: The Son Also Rises," *Asian Survey*, Vol. 21, No. 1 (January 1981), p. 113.
- <sup>121</sup> Lim, *Kim Jong Il's Leadership of North Korea*, pp. 52-53.
- <sup>122</sup> Lim, *Kim Jong Il's Leadership of North Korea*, pp. 52-57.
- <sup>123</sup> Weber, "The Three Types of Legitimate Rule," pp. 6-8.
- <sup>124</sup> Mike Chinoy, *Meltdown, The Inside Story of the North Korean Nuclear Crisis* (New York: St. Martin's Press, 2008), p. 33.
- <sup>125</sup> Peter G. Northouse, *Leadership*, 7th ed., p. 99.
- <sup>126</sup> Daniel Tudor and James Pearson, *North Korea Confidential: Private Markets, Fashion Trends, Prison Camps, Dissenters and Defectors* (Rutland, VT: Tuttle Publishing, 2015), pp. 90-91. The Three Revolutionary Movement focused on cultural, technical, and ideological aspects of North Korean society to strengthen the regime. Unlike China's Red Guards, the center (i.e., Kim Jong-il) controlled the movement.
- <sup>127</sup> Bruce E. Bechtol, Jr., *The Last Days of Kim Jong-Il, The North Korean Threat in a Changing Era* (Dulles, VA: Potomac Books, 2013), pp. 59-61.
- <sup>128</sup> Choe Sang-hun, Shin Gi-Wook, and David Straub, *Troubled Transition: North Korea's Politics, Economy, and External Relations* (Stanford, CA: The Walter H. Shorenstein Asia-Pacific Research Center, 2013), pp. 48-51.



- <sup>129</sup> Andrei Lankov, "Kim Jong Un's popularity, explained," NK News.Org, September 27, 2015, <http://www.nknews.org/2015/09/kim-jong-uns-popularity-explain/> (accessed September 27, 2015).
- <sup>130</sup> Lim Dong-won, *Peacemaker: Twenty Years of Inter-Korean Relations and the North Korean Nuclear Issue* (Stanford, CA: Walter H. Shorenstein Asia-Pacific Research Center, 2012), p. 64.
- <sup>131</sup> Lim, *Peacemaker*, p. 64.
- <sup>132</sup> Yoichi Funabashi, *The Peninsula Question: A Chronicle of the Second Korean Nuclear Crisis* (Washington, DC: Brookings Institution Press, 2007), pp. 178-179.
- <sup>133</sup> Madeleine Albright, *Madam Secretary, A Memoir* (New York: Miramax Books, 2003), pp. 466-469.
- <sup>134</sup> Chinoy, *Meltdown*, p. 33.
- <sup>135</sup> Grisafi, "Kim Jong Un may be easing reign of terror over elites."
- <sup>136</sup> Choe, Shin, and Straub, *Troubled Transition*, pp. 47-49.
- <sup>137</sup> Bruce Klingner, "North Korea Heading for the Abyss," *Washington Quarterly*, Vol. 37, No. 3, Fall 2014, pp. 175-176.
- <sup>138</sup> Bruce Cumings, "The Kims' Three Bodies," pp. 217-218.
- <sup>139</sup> Lankov, "Kim Jong Un's popularity, explained."
- <sup>140</sup> Lankov, "Kim Jong Un's popularity, explained."
- <sup>141</sup> Don Oberdorfer and Robert Carlin, *The Two Koreas: A Contemporary History*, revised and updated, 3<sup>rd</sup> ed. (New York: Basic Books, 2014), pp. 454-455.
- <sup>142</sup> Andray Abrahamian, "The ABCs of North Korea's SEZs," U.S.-Korea Institute (2014), pp. 7-13.
- <sup>143</sup> Constitution of the Democratic People's Republic of Korea (2012), [https://en.wikisource.org/wiki/Constitution\\_of\\_the\\_Democratic\\_People%27s\\_Republic\\_of\\_Korea\\_\(2012\)](https://en.wikisource.org/wiki/Constitution_of_the_Democratic_People%27s_Republic_of_Korea_(2012)) (accessed July 12, 2015).
- <sup>144</sup> Lee Hong Yung, "North Korea in 2013: Economy, Executions, and Nuclear Brinkmanship," *Asian Survey*, Vol. 54, No. 1 (2014), pp. 91-92.
- <sup>145</sup> KCNA, "KCNA Commentary Warns U.S., S. Korean Warmongers Not to Wage War Drills Targeting DPRK's Headquarters and Social System," March 7, 2013, <http://www.kcna.us/2013/03/07/news-14/> (accessed September 26, 2015).
- <sup>146</sup> KCNA, "New Strategic Line, Succession of Line of Simultaneously Developing Economy and Defense," April 1, 2013, <http://www.kcna.us/2013/04/02/news-27/> (accessed September 26, 2015).
- <sup>147</sup> KCNA, "New Strategic Line, Succession of Line of Simultaneously Developing Economy and Defense."
- <sup>148</sup> KCNA, "US, S. Korea to Be Held Accountable for Catastrophic Consequences," March 11, 2013, <http://www.kcna.us/2013/03/11/news-29/> (accessed September 26, 2015).
- <sup>149</sup> KCNA, "DPRK People in War Posture," March 11, 2013, <http://www.kcna.us/2013/03/11/news-24/> (accessed September 26, 2015).
- <sup>150</sup> KCNA, "DPRK Servicepersons Inspired by Kim Jong Un's Inspection," March 12, 2013, <http://www.kcna.us/2013/03/12/news-24/> (accessed September 26, 2015).
- <sup>151</sup> KCNA, "[Law on Consolidating Position of Nuclear Weapons State Adopted](http://www.kcna.us/2013/04/01/news-23/)," April 1, 2013, <http://www.kcna.us/2013/04/01/news-23/> (accessed September 26, 2015).
- <sup>152</sup> Lee Hong Yung, "North Korea in 2013: Economy, Executions, and Nuclear Brinkmanship," *Asian Survey*, Vol. 54, No. 1 (2014), pp. 92-93.
- <sup>153</sup> Dan Roberts and Justin McCurry, "U.S. defends military deployments in response to North Korea threats," *The Guardian*, April 4, 2013, <http://www.theguardian.com/world/2013/apr/04/us-north-korea-military-response> (accessed July 13, 2015).
- <sup>154</sup> Jill Dougherty, "Kerry visits South Korea amid North Korea's nuclear threats," CNN, April 11, 2013, <http://www.cnn.com/2013/04/11/world/asia/south-korea-kerry-trip/> (accessed July 14, 2015).
- <sup>155</sup> KCNA, "Nuclear Deterrence Serves as Treasure Common to Nation: Rodong Sinmun," May 13, 2013, <http://www.kcna.us/2013/05/13/news-07/> (accessed September 26, 2015).
- <sup>156</sup> KCNA, "Nuclear Deterrence Serves as Treasure Common to Nation."
- <sup>157</sup> KCNA, "Park Chung-hee and His Daughter Accused of Sycophancy toward Japan," August, 4, 2015, <http://kcna.watch.nknews.org/article/fbsu> (accessed September 27, 2015).
- <sup>158</sup> KCNA, "Park Chung-hee and His Daughter Accused of Sycophancy toward Japan."
- <sup>159</sup> KCNA, "Park Chung-hee and His Daughter Accused of Sycophancy toward Japan." 300 million yen is about \$2,564,100 at \$117 yen to the dollar exchange rate.
- <sup>160</sup> KCNA, "Park Chung-hee and His Daughter Accused of Sycophancy toward Japan."
- <sup>161</sup> Kathy Novak, "North Korea sets clocks back 30 minutes creating its own time zone," CNN, August 13, 2015, <http://www.cnn.com/2015/08/07/asia/north-korea-time-zone/> (accessed August 28, 2015).
- <sup>162</sup> KCNA, "Pyongyang Time Newly Fixed in DPRK," August 6, 2015, <http://kcna.watch.nknews.org/article/fbvy> (accessed September 27, 2015).
- <sup>163</sup> KCNA, "Spokesman for CPRK Slams Park Geun Hye's 'Address on August 15'," August 16, 2015, <http://kcna.watch.nknews.org/article/fcn7> (accessed September 27, 2015).
- <sup>164</sup> Anna Fifield, "S. Korea agrees to end broadcasts as North expresses regret for provocations," *The Washington Post*, August 24, 2015, [https://www.washingtonpost.com/world/asia\\_pacific/north-korea-hates-those-loudspeakers-because-they-make-fun-of-kim/2015/08/24/439f6039-3f37-490b-9fa1-e3b8022893e6\\_story.html](https://www.washingtonpost.com/world/asia_pacific/north-korea-hates-those-loudspeakers-because-they-make-fun-of-kim/2015/08/24/439f6039-3f37-490b-9fa1-e3b8022893e6_story.html) (accessed August 24, 2015).
- <sup>165</sup> KCNA, "Kim Jong Un Guides Emergency Enlarged Meeting of WPK Central Military Commission," August 21, 2015, <http://kcna.watch.nknews.org/article/fcrr> (accessed September 27, 2015).
- <sup>166</sup> Park Ju-min and Tony Munroe, "Tensions rise as North and South exchange fire," August 20, 2015, <http://www.reuters.com/article/2015/08/21/us-northkorea-southkorea-artillery-idUSKCN0QP0RO20150821> (accessed August 29, 2015).
- <sup>167</sup> Ashley Rowland and Yoo Kyong Chang, "Agreement to ease Korea tensions raises hope of better relations," *The Stars and Stripes*, August 25, 2015, <http://www.stripes.com/news/agreement-to-ease-korea-tensions-raises-hope-of-better-relations-1.364501> (accessed September 26, 2015).
- <sup>168</sup> Fox News, "South Korea vows response to 'provocations' from North after exchange of fire," August 21, 2015, <http://www.foxnews.com/world/2015/08/21/nkorea-warns-war-after-exchange-fire-with-south/> (accessed October 2, 2015).
- <sup>169</sup> Fifield, "S. Korea agrees to end broadcasts as North expresses regret for provocations."
- <sup>170</sup> Rowland and Yoo, "Agreement to ease Korea tensions raises hope of better relations."
- <sup>171</sup> Grisafi, "Kim Jong Un may be easing reign of terror over elites."
- <sup>172</sup> Grisafi, "Kim Jong Un may be easing reign of terror over elites."
- <sup>173</sup> Grisafi, "Kim Jong Un may be easing reign of terror over elites."

<sup>174</sup> Scott Snyder, "North Korea Currency Reform: What Happened and What Will Happen to Its Economy?" paper presented at 2010 Global Forum on North Korea Economy, Korea Economic Daily and Hyundai Research Institute, Seoul, Korea, March 31, 2010, pp. 1-4.

<sup>175</sup> KCNA, "WPK Central Committee Issues Order to Conduct First H-Bomb Test," January 6, 2016, <http://www.kcnawatch.co/newstream/1452124924-138163682/wpk-central-committee-issues-order-to-conduct-first-h-bomb-test/> (accessed January 9, 2016).

<sup>176</sup> Anna Fifield, "Not all of N. Korea's weapons buildup is nuclear," *The Washington Post*, June 9, 2016, p. A10.

<sup>177</sup> Anna Fifield, "Not all of N. Korea's weapons buildup is nuclear."

<sup>178</sup> Cha Du-hyeogn, "North Korea balances threats with promises at the Seventh Congress," May 20, 2016, <https://www.nknews.org/2016/05/north-korea-balances-threats-with-promises-seventh-congress/> (accessed May 11, 2016).

<sup>179</sup> Nye, *The Future of Power*, p. 212.

*Dr. David W. Shin is a faculty member in the Department of Regional Intelligence Issues, College of Strategic Intelligence, National Intelligence University. He served over 25 years in the U.S. Army's Military Intelligence Corps and as a Northeast Asia Foreign Area Officer, retiring in 2011 as a Colonel. He holds a PhD from Cranfield University, Defence Academy of the United Kingdom, and master's degrees from the then-Defense Intelligence College (now NIU), the University of Washington, and the then-Industrial College of the Armed Forces (now Eisenhower School) at National Defense University. He graduated from Virginia Military Institute in 1986.*



## KIERNAN GROUP HOLDINGS

EXCEPTIONAL INTELLIGENCE TRADECRAFT AND  
LAW ENFORCEMENT STREETCRAFT

+

EXTENSIVE OPERATIONAL EXPERIENCE

=

## GAME-CHANGING SOLUTIONS

CRAFTY BASTARDS® STRATEGIES – ACTIVE THREAT WORKSHOPS –  
GLOBAL FUSION – EMERGING TECHNOLOGY INNOVATION CENTER®

[www.kiernan.co](http://www.kiernan.co) – 571-290-0260

---

# The Moral-Ethical Domain and the Intelligence Practitioner

by LTC (USAR, Ret) Christopher E. Bailey

---

## AN EMERGING PROFESSIONAL IDENTITY

The work of intelligence practitioners has been the focus of much public debate and controversy over the past ten years, with many people questioning the moral/ethical propriety of a wide range of intelligence activities. One could ask, for example, whether Director James Clapper “lied” to the Congress when he gave the “least untruthful answer” to a question from Senator Ron Wyden (D-OR) or whether National Security Agency contractor Edward Snowden committed a moral/ethical violation in making his disclosures to *The Guardian* (assuming that he actually revealed illegal activities).<sup>1</sup> Indeed, some earlier voices aptly called for a code of professional ethics to “enable practitioners to define their responsibilities, provide guidance, inspire, motivate, raise awareness and consciousness, as well as improve the quality and consistency of the work they perform.”<sup>2</sup> In that respect, a strong ethical framework should serve as a compass in guiding intelligence practitioners in unique issues not readily apparent to the public, or even subject to regular oversight.

Typically, proffered codes have explored partial views (often with a mission focus), to include compliance with regulatory standards (e.g., international treaties, domestic statutes or executive orders) or in “speaking truth to power” (e.g., the problem with politicized intelligence). Some proposals have demanded limits on practitioner support to controversial activities, such as enhanced interrogation (torture), renditions, electronic surveillance, and covert operations. Jan Goldman argues more generally that a code should define acceptable behavior, promote high standards of practice, provide a benchmark for member self-evaluation, and establish a framework for daily behavior, to be used as a vehicle for occupational identity and to mark occupational maturity.<sup>3</sup> In other words, a broadly stated ethical framework is important in terms of professional identity *per se* with the intelligence practitioner acting as a moral agent.

This issue of professional identity has taken on increased importance in light of the passage of the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), which created the Office of the Director of National

Intelligence (ODNI) and generally fostered greater integration and collaboration in the Intelligence Community (IC).<sup>4</sup> Here, the IC has made great strides with increased emphasis on Community-wide integration with aspirational and regulatory standards relating to mission management; standards of conduct; the selection, retention, and promotion of personnel; tradecraft standards and practices; and training and education. The DNI has also set a 2006 vision for ethical conduct, calling for “an *Ethos* of Service, Integrity, and Accountability.”<sup>5</sup> The DNI then defines that *Ethos* as the “code” of shared values that guides the way an individual (and an organization) behaves, and defines an institution’s culture. In any case, the DNI *Ethos* results from both legal and moral sources that help define who intelligence practitioners “should” be and what we should/should not do.<sup>6</sup>

One way to view this effort is in terms of how the DNI sees the senior practitioner. Intelligence Community Directive (ICD) 610-1, the Core Qualification Standard for Senior Civilian Officers in the Intelligence Community, establishes and defines validated core competencies applicable to all IC senior officers, including the IC-specific “joint” competencies: Collaboration and Integration, Enterprise Focus, and Values-Centered Leadership.<sup>7</sup> This effort at greater professionalization is also evident in the IC joint duty program, a civilian personnel rotational system designed to encourage and facilitate assignments and details of personnel to national intelligence centers and between elements of the intelligence community.<sup>8</sup> Clearly, the Community is moving in the right direction in terms of professional identity, standards of practice, benchmarks for individual and organizational development, and behavioral norms. In fact, the work of intelligence practitioners is in the process of evolving into a profession as that term has been applied to long-standing and well-integrated professions such as medicine or law.

In 2013 the DNI promulgated seven ethical principles that are expected to guide intelligence practitioners in their daily work.<sup>9</sup> Initially, the DNI recognizes that practitioners serve in a unique profession, and—as

such—should have a code of ethics that guides our work. This is, according to the DNI, “because we [intelligence officers] have unique access and training, so we’re capable of reaching informed decisions when the general public can’t, and that’s true across the IC.”<sup>10</sup> He then goes on to say that “on top of that academic reasoning, I felt that a professional ethical code was necessary because we live in a classified world, where the details of even our oversight are secret, and so it is even more important for us to hold ourselves accountable.” Second, the set of principles is striking for its inclusion not simply in the 2014 *National Intelligence Strategy*, but for its prominent placement in that document: The DNI clearly deems the ethical principles to be a key part of national intelligence, such that they would be featured—not in an appendix—but in the opening pages of the *National Intelligence Strategy*. Clearly, the DNI has created a very important foundational document for the Intelligence Community; this document provides a starting point for further work.

- Truth: We seek the truth; speak truth to power; and obtain, analyze, and provide intelligence objectively.
- Lawfulness: We support and defend the Constitution, and comply with the laws of the United States, ensuring that we carry out our mission in a manner that respects privacy, civil liberties, and human rights obligations.
- Integrity: We demonstrate integrity in our conduct, mindful that all our actions, whether public or not, should reflect positively on the Intelligence Community at large.
- Stewardship: We are responsible stewards of the public trust; we use intelligence authorities and resources prudently, protect intelligence sources and methods diligently, report wrongdoing through appropriate channels; and remain accountable to ourselves, our oversight institutions and, through those institutions, ultimately to the American people.
- Excellence: We seek to improve our performance and our craft continuously, share information responsibly, collaborate with our colleagues, and demonstrate innovation and agility when meeting new challenges.
- Diversity: We embrace the diversity of our Nation, promote diversity and inclusion in our work force, and encourage diversity in our thinking.

This level of generality is useful in that it provides overall direction without becoming “rule-based”; still, the principles lack an integrated view of the practitioner’s

daily work. The principles obscure some important issues, such as the nature of the client relationship, standards of practice, and professional relationships among practitioners. Moreover, the principles do not address other issues that practitioners face.

Government employees, both military and civilian, have evidenced a growing number of ethical problems over the past ten years.<sup>11</sup> In general, government employees have faced ethical challenges in many important areas to include personnel decisions, such as the hiring of new employees, promotion decisions, annual performance evaluations and bonuses; the handling of workplace complaints regarding harassment or discrimination based upon sex, ethnicity, or other protected status; the stewardship over government resources, perhaps involving travel claims or the use of telework; inappropriate senior-subordinate relationships; conflicts of interest in procurement actions; the appropriate use of contractors; and the handling of Inspector General complaints and possible reprisal actions.<sup>12</sup> One earlier, classic case involves Ernest Fitzgerald, who exposed mismanagement in the C-5 Galaxy aircraft program in his 1969 testimony before the U.S. Congress. Fitzgerald was then forced to leave government, and later found that the Nixon administration had gone to lengths to discredit him and have him terminated for having divulged “classified” information. Indeed, some would argue that is it in the area of promotions and performance appraisals that management is most clearly tested on ethics and integrity.

---

***The DNI principles neglect the important obligation of senior professionals to educate and mentor subordinates.***

---

IC employees often face unique low-visibility issues, many of which are not shared by other federal employees and typically take place outside public scrutiny. In other words, while intelligence professionals are obligated to follow the general rules promulgated by the Office of Government Ethics, those rules are necessary but not sufficient for intelligence practitioners. In that respect, the Principles of Professional Ethics promulgated by the DNI are an important step that advances the professional identity of intelligence practitioners. Intelligence practitioners may be challenged with biased collection reports, the propriety of inflated evaluations on intelligence reports, giving someone unwarranted co-author credit on an analytic product, the mishandling and/or misuse of classified information, the reporting of derogatory information to a security investigator (e.g., withholding unflattering information about a colleague going through a clearance update), contacts with foreign nationals or members of the media (e.g., leaks to the



press for self-gain), gifts from/to foreign contacts, and the use of IC employment for self-gain. Some practices are regulated by law, while others involve judgment calls.<sup>13</sup> In any case, sound ethical practices enhance organizational cohesion and advance mission accomplishment. Unethical practices impair trust at both a personal and an organizational level.

A framework for professional ethics should consider the full range of conceptual issues relating to professional practice *per se*, that is issues such as relationships with policy clients, the standard of care, due diligence in developing/rendering necessary professional expertise, relationships among practitioners, and integrity in general. The DNI principles neglect the important obligation of senior professionals to educate and mentor subordinates. The principles could better explain how diversity supports collaboration and team learning. Overall, a renewed focus on ethics is important in terms of professional identity and performance at the individual level, as well as fostering the emergence of a “learning organization” at the agency level.

## THE NATURE OF THE PROFESSION

The DNI principles, as well as the earlier DNI Ethos, are consistent with the view that intelligence is a “profession” within the meaning advanced by the political scientist Samuel Huntington in 1957.<sup>14</sup> Huntington identified the three essential attributes of a profession as responsibility, corporateness, and expertise. In one sense, a code of ethics can be a critical system that can help establish professional obligations to clients and other practitioners, set benchmarks for performance, and foster an enhanced professional identity. Some professions such as medicine or law, with tightly controlled education, licensing, and disciplinary processes, are well regulated in the interests of protecting the public (e.g., either the patient or the client) from the predatory/negligent practitioner. Intelligence is an emerging profession with a unique identity that has important and far-reaching obligations. Such a code would enhance trust in the profession and in practitioners in general. In that sense, a well-considered code would also help protect the American people, as well as the profession itself, from negligent practitioners.

Stewardship—the responsible discharge of duty and management of resources entrusted to our care for the benefit of others—is the most important hallmark of a professional. We serve, as responsible practitioners, not for self-gain but to advance the national security interests of the American people acting through the President and elected/appointed officials in government. We have an overriding duty to provide timely, accurate, and relevant support to policymakers, free from partisan political bias.<sup>15</sup> The nature of our calling, as well as the demands of secrecy, demand a

high standard of care (the skill and due diligence expected of a practitioner) in our daily work.<sup>16</sup> We balance competing demands to advance national security, consistent with American values and law, with a requirement to maintain a level of transparency and accountability to the American people. At all times, we must maintain public trust through our protection of sources and methods, our use of resources, and our accountability for mission success/failure. We are moral agents, ultimately accountable to the American people, for our daily judgments based on American values.

---

### *The intelligence practitioner has broad obligations in terms of advice and support to the policymaker.*

---

What is the nature of the practitioner-policymaker “client” relationship? Does the policymaker serve as a client, a customer, or a consumer? Does the practitioner serve as a deliveryman of news, analysis, and expertise, or as something more? In fact, the practitioner is duty-bound to support the policy client. A client relationship implies a principal-agent relationship with the policymaker maintaining authority, direction, and control, while the autonomous intelligence officer provides a confidential service, all within the context of a trust relationship. This view sees the intelligence practitioner as much more than the purveyor of information to a “reader.” This view also implies that the policymaker has an obligation to provide more than just his information needs; the fully empowered practitioner must know the client’s policy objectives, priorities, concerns, and possible course of action, if that practitioner is to provide a fully effective service.

The intelligence practitioner has broad obligations in terms of advice and support to the policymaker. Paul Miller, a former member of the National Security Council staff, explained: “The IC cannot recommend policy, but it can provoke thought, present scenarios, and explore implications for U.S. interests under different assumptions.”<sup>17</sup> This also means that intelligence officers will also be party to many client confidences, not necessarily classified, all of which must be protected from peremptory public disclosure. Nonetheless, a close relationship between the policymaker and the intelligence professional will involve many subtle and challenging situations, with concerns about differing agendas and mindsets, pressures to conform intelligence reporting to support policy preferences, and a possible loss of objectivity on the part of intelligence practitioners.<sup>18</sup> On one hand, the practitioner can use a close professional relationship to provide timely insights that help the policymaker understand a complicated, nuanced and

ambiguous situation. On the other hand, such a relationship will help the policymaker understand what the intelligence community can and cannot realistically do.

The practitioner-policymaker relationship is undoubtedly the key to understanding to our professional identity; as intelligence practitioners we exist to provide support—a decision advantage—to national security policy officials.<sup>19</sup> The nature of this relationship has also been at the forefront of much public debate in recent years, largely amid charges of “politicized” intelligence and concerns about timely, relevant products. There have long been two schools of thought, one that traces its origins to Sherman Kent, who adamantly contended that intelligence analysis provides a service to policymakers and should not be involved in the formulation of policies, and the alternative view that a strict separation deprives policymakers of the insights that an informed officer can provide.<sup>20</sup> In the first view, some have feared that “objective” analysis could become tainted by proximity to the policy process. The proponents here argue that a “firewall” is needed to ensure that intelligence products do not serve partisan ends.

---

*There have long been two schools of thought, one that traces its origins to Sherman Kent, who adamantly contended that intelligence analysis provides a service to policymakers and should not be involved in the formulation of policies, and the alternative view that a strict separation deprives policymakers of the insights that an informed officer can provide.*

---

In the second view, others have been concerned that if practitioners maintain a strict separation from policymakers we would have less understanding about our customers and their needs. The supporters argue that a close relationship is needed to ensure that work product is relevant to client requirements. In any case, the practitioner needs prompt feedback on the timeliness, accuracy, and relevance of the service he provides. Surely, no matter how one sees this relationship, the practitioner must understand the dynamic needs and interests of the policymaker, while maintaining a dialogue based upon trust.

Josh Kerbel argues that intelligence professionals should see themselves as a service provider with a client relationship based upon trust, not necessarily on the provision of accurate information *per se*.<sup>21</sup> This view recognizes that intelligence professionals can provide an

important service to clients in terms of examining and using the available evidence, even if one cannot always be right in his assessments. Kerbel argues that intelligence practitioners must be closer to the clients they serve. He offers that policymakers “could explore policy ideas, tap into the expertise of the IC about possible consequences of a policy—potential downsides on unanticipated benefits.”<sup>22</sup> He sees the intelligence officer as “synthesizing” with clients: “Analysts would thus provide the elements that could be combined in imaginative ways to create something new, a process the Greeks say is the antithesis of analysis, or *synthesis*.”<sup>23</sup> Moreover, policymakers would be much better informed about the strengths and limitations of the intelligence enterprise. This useful approach means that intelligence officers would work together as an integrated team supporting the client with a service that factors in the effect of U.S. actions and policies on their work.

We often hear that intelligence practitioners have an obligation to “speak truth to power,” the truth and integrity points in the ODNI principles. The truth can be uncomfortable; superiors may or may not have the patience to take criticism from a subordinate. How does the “loyal” practitioner proceed in such a situation? What is the role of constructive dissent for the intelligence officer? Yes, an officer can proceed in a tactful manner, privately offering a “perspective,” “context,” or even the possible second/third-order consequences of a decision. Yes, a superior can offer the “big picture”—often a good leadership practice that helps maintain group communications and cohesion—helping the subordinate appreciate things not otherwise apparent. And yet, sometimes neither the efforts of subordinates nor seniors are sufficient in bridging the gap. How does an ethical intelligence officer proceed in that situation? While intelligence practitioners can use whistleblower channels, to include reporting to the Inspector General or the Congressional oversight committees, many question the effectiveness of such approaches.<sup>24</sup> Indeed, the Intelligence Community lacks a culturally accepted tradition or process such as the State Department’s dissent channel that even features annual awards.

One important issue relates to the “jurisdiction” of the intelligence profession. Is the profession limited to collectors, analysts, and their senior managers who brief the policy clients? Or does the profession include the myriad of human capital, information technology, and logistics officers, along with the supporting cast of staff officers and clerks, who comprise the modern government agency? One could analogize the intelligence profession to the practice of law or medicine. In that respect, while the lawyer is supported by a “professional” office staff that does many things for the client, only the lawyer is permitted to appear in court and represent that client “before the bar.” Both lawyers and physicians have a level of autonomy—

independence in making certain decisions for the client/patient—that cannot be extended to the supporting staff. This restricted view is based on the practitioner’s responsibility and exclusive authority to act on behalf of the client/patient. In short, the practitioner owes a duty to the client/patient that is not fully shared with the professional staff.

In the alternative, one could adopt a unitary view that embraces the range of intelligence disciplines under a “big tent” theory. As an example, Huntington once viewed the military profession as including officers, but neither noncommissioned officers nor junior enlisted personnel. Yet few people still subscribe to that non-egalitarian 1957 view based upon the change from a conscript (drafted) force structure to an all-volunteer service with rising levels of education and technological sophistication. Today, we have a noncommissioned officer corps that is profoundly different from its forebears. Indeed, both commissioned and noncommissioned officers have many shared mission-oriented obligations: if the platoon leader is killed on the battlefield, the platoon sergeant is expected to take command and continue the fight.

Intelligence practitioners should undoubtedly focus on the elements that bring us together as a like-minded community with a common mission, shared values, and complementary knowledge, skills, and attributes. One writer, addressing the jurisdiction of the military profession, cautions that choices have long-term meaning: “If we can define our profession in ways that society will accept and trust, we will remain viable and relevant. Doing so demands defining our professional expertise, contesting control of it when required, and being clear about who exercises authority and responsibility delegated to us by society.”<sup>25</sup> There is great merit in recognizing the integrated team, with practitioners from different occupational groups (guilds, if you will) providing discrete tradecraft contributions, no matter who actually represents the community in meeting with the policy client.

## THE INTELLIGENCE AGENCY AS A LEARNING ORGANIZATION

The intelligence agency, as a learning organization, should exhibit certain important characteristics in terms of meeting the diverse, uncertain, and volatile threats to U.S. national security. Peter Senge, Director of Systems Thinking and Organizational Learning at the Massachusetts Institute of Technology (MIT) Sloan School of Management, contends that learning organizations exhibit five main characteristics: systems thinking, personal mastery, mental models, a shared vision, and team learning. He sees the principal role of the leader as a designer, focused on the governing ideas of purposes, vision, and core values by which people will live, with a mandate to

engage people at all levels. Leaders serve as teachers, “helping people achieve more accurate, more insightful, and more *empowering* views of reality.”<sup>26</sup> Senge contends that learning organizations are built by communities of servant leaders, “people who lead because they choose to serve, both to serve one another and to serve a higher purpose.”<sup>27</sup> Arguably, given our mission in the defense of the nation, the intelligence agency should be the *sine qua non* of a learning organization, with an ever-increasing understanding of and adaptation to the changing world in which we live. We cannot wait for client requirements to drive our work; we must be proactive in anticipating the needs of our policy clients.

---

***...the intelligence agency should be the sine qua non of a learning organization, with an ever-increasing understanding of and adaptation to the changing world in which we live. We cannot wait for client requirements to drive our work; we must be proactive in anticipating the needs of our policy clients.***

---

We should create a learning environment as a means of enhancing organizational capacity and mission accomplishment. Edgar Schein, a former MIT professor who made a notable mark on the field of organizational development, contends that a psychologically safe environment is required; this environment should include opportunities for training and practice, support in overcoming past errors, coaching and rewards for work in a positive direction, norms that legitimize the making of errors, and norms that reward innovative thinking and experimentation.<sup>28</sup> A safe learning environment facilitates creativity and innovation. Practitioners must value learning, both in terms of personal development through a range of activities as well the organizational learning that results from the contributions of colleagues.

Diversity is an important means to this end. Business professors David Thomas and Robin Ely identify three dominant paradigms that have guided most diversity initiatives: discrimination-and-fairness, access-and-legitimacy, and learning effectiveness.<sup>29</sup> Under the first perspective, they argue that leaders have often focused on issues such as equal opportunity, fair treatment, recruitment, and compliance with federal laws. Under the second perspective, companies seek diversity as a means of accessing and establishing legitimacy with consumer groups. They argue, however, that leaders should combine the two perspectives in a learning effectiveness paradigm

which recognizes the varied perspectives and approaches that members of different identity groups bring to work. They say that companies using this approach “have also developed an outlook on diversity that enables them to *incorporate* employees’ perspectives into the main work of the organization and to enhance work by rethinking primary tasks and redefining markets, products, strategies, missions, business practices, and even cultures.”<sup>30</sup>

Diversity allows for a richer, more collaborative working environment; we grow as a team—not through competition for either recognition or resources—but through cooperation.<sup>31</sup> It is through respect for others that we bring together a team that works on a collaborative basis, infusing all that we do with the perspectives and contributions of others. We must acknowledge that we learn from others with contrarian views, just as much as we learn from “research.” This view focuses on the accomplishments not of practitioners, but of teams, groups, and the community itself. This view permits an organization to adapt and respond to new challenges with great agility. In this manner, an intelligence team that includes the diverse backgrounds normally associated with the ethnic, gender, and age groups traditionally protected by law, as well as varied educational,

work, and life experiences, can function as a true collaborative organization to achieve a greater understanding of the problems facing us. Again, mutual respect is the glue that holds this organization together.

Systems thinking is critical in the area of professional ethics. First, and most important, senior leaders create the conditions, including both the organizational culture and climate, necessary for professional practice. Senior leaders must set performance standards and hold subordinates accountable in meeting national security requirements on behalf of the policy client. Second, we have an obligation to consider ethics in a holistic manner, one that addresses all aspects of professional activities. Third, senior leaders have an obligation to mentor and develop subordinates in a constructive manner toward clear, objective goals. Intelligence practitioners should view ethics through the full range of professional duties to include relationships with the policy client, the standards of practice, and acceptable behaviors among practitioners. This view should help promote professional identity and provide a benchmark for member self-evaluation.

What are the ethical duties for the intelligence professional?

ETHICAL CANONS FOR INTELLIGENCE PROFESSIONALS		
ETHICAL CANON	KEY ISSUES	KEY POINTS
Duty of Candor	Duty is owed to superiors, co-workers, and subordinates; this duty speaks to the practitioner’s sense of integrity and permits a degree of dissent with seniors.	Speaking truth when called for; breach can occur by omission or commission; duty requires certain independence in providing constructive advice and support.
Duty of Confidentiality	Duty is owed to client (policymaker) to protect (policy) confidences and act on non-partisan basis; duty is owed co-workers & subordinates on privacy issues.	Protects client (trust) relationship; DNI serves as advisor to the President, 50 U.S.C. §403 (b) (2). Promotes respect in workplace and with the public.
Duty to Disclose	Fiduciary obligation per PPD 19; failure to do so can lead to imprisonment.	Fraud, waste, and abuse; criminal activity; security vulnerabilities and violations; and whistle-blowing.
Duty of Due Diligence (the Standard of Care in Professional Practice)	Practitioner is obligated to develop knowledge, skills, and attributes required for assigned missions and tasks; practitioner must collaborate with other professionals to ensure policy client is provided the full range of diversified expertise.	Practitioners participate in lifelong learning activities, to include job training, self-development, and networking activities; diversity promotes organizational learning and effectiveness. Joint development activities enhance the sense of profession.
Duty of Mentorship	Duty is owed by seniors to subordinates; mentorship occurs on formal and informal basis.	Seniors pass on knowledge, skills, and attributes; this facilitates judgment in others.
Duty to Protect Sources & Methods	Fiduciary obligation; 50 U.S.C. §403-1 (i).	Protects classified information; this duty impacts media contacts, pre-publication review, and whistle-blowing activities.
Duty of Respect	Duty is owed to superiors, co-workers, and subordinates.	Treat others as co-professionals, without regard to ethnicity, gender, age, or other protected category; give credit to others where it is due and avoid passing blame for own shortcomings.
Duty of Stewardship	Broad sense of responsibility to policy client in discharging duties.	Proper use of government resources/funds; non-use of position for private gain.



---

## DEVELOPING PERSONAL MASTERY IN OTHERS

“**M**entor took the floor, Odysseus’ friend-in-arms to whom the king, sailing off to Troy, committed his household, ordering one and all to obey the old man and he would keep things steadfast and secure.”<sup>32</sup> The modern term “mentor,” often reflecting a relationship between a more experienced person and someone with lesser experience, originates from the poetic lines in which Mentor, and friend of Odysseus’ father, was left to oversee Odysseus’ home while Odysseus himself went to war. In fact, senior intelligence practitioners have an ethical obligation to help subordinates grow through a similar transfer of knowledge, skills, and judgment. Indeed, this transfer helps shape junior personnel to the IC’s core values of Commitment, Courage, and Collaboration.<sup>33</sup> Intelligence leaders must mentor others in the critical thinking skills that can help them address ethical problems; leaders must foster personal mastery in others as a means building greater organizational capacity.

Peter Senge argues that most leaders are skilled at articulating their own views and presenting them persuasively (advocacy). He notes that, while such skills are important, it is equally important that senior leaders possess *both* advocacy and inquiry skills as they confront the increasingly complex issues that come with increased responsibility within an organization. Here, intelligence practitioners often face unique ethical dilemmas, the “right vs. right” issues, which can be the result of two deeply held yet opposing values in an ambiguous, time-sensitive situation. And, when considering a subordinate’s past actions, a senior leader must seek to understand the other person’s point of view, rather than simply restating his own confrontational view of what should or should not have been done. An effective mentor must engage in a dialogue, with open-ended questions, to tease out what was understood to be the dilemma.<sup>34</sup> This process helps leaders deal with each ethical situation on its own specific merits.

### *Eliciting the Dilemma*

- What were understood to be the issues and values at stake?
- What information (facts, not opinions or beliefs) was known to the subordinate?
- What assumptions and inferences were made?
- What resources (people, documents) were consulted in the decision-making process?
- How did the subordinate assess the moral/ethical issues that were presented (e.g., what theories and concepts were considered)?
- What were the alternative solutions that could have been applied to this problem?

---

## ELICITING THE DILEMMA

**S**ome problems are not real dilemmas at all, perhaps because the right answer is clear (although distasteful or not the preferred course of action), or because the conflict can be resolved through a precise definition of the facts or in the sequencing of actions. For example, was time really a constraint or should one value have been prioritized over another? Is there a “big picture” that the subordinate might be missing? In any case, we need to help subordinates “unpack” the intuitive, if not emotionally laden, decision-making that comes with many moral/ethical issues, helping subordinates adopt more appropriate mental models and develop an appreciation for the nuances and consequences of our decisions.<sup>35</sup>

---

*Senior leaders must be willing to accept some degree of dissent, as well as show some acceptance of “honorable” failure.*

---

Senior leaders must be willing to accept some degree of dissent, as well as show some acceptance of “honorable” failure. We must encourage subordinates to speak frankly about how they perceive situations and how they make decisions. On one hand, if respectful dissent is seen as a lack of loyalty or a challenge to authority, we won’t create a healthy work environment. We will leave people feeling like they can’t talk to the boss, that it is better to leave some things unsaid, or that they can’t exercise their own authority. On the other hand, if subordinates feel that they can raise important issues, with a resulting dialogue that produces meaningful feedback for both the senior and the subordinate, we can then create a learning environment that is focused on mission accomplishment and advances core values. Professionals can and should test limits when acting in good faith to further a policy client’s interests—“playing with chalk on the cleats.” Mistakes should be seen “as an opportunity for learning and growth, rather than as cause for punishment and permanent stigmatization.”<sup>36</sup>

The elicitation process allows the senior leader to understand what the subordinate was thinking and to help reshape that person’s mental models consistent with the IC’s core values. I call this process “diagnosing the problem before prescribing the treatment.” After all, who would trust a physician who began by handing out medicine, rather than asking some tough questions and running some diagnostic tests? Truly, unless a mentor engages the subordinate in a meaningful, respectful way, we lose an important opportunity to teach ethical problem-solving and to foster individual development.

The point, especially as it applies to professional ethics, is that it is more important to teach people how to think, rather than just hammer home the fact that we think they made a mistake. The senior leader must create a psychologically safe environment, both one that tolerates some level of failure as well as one that permits a healthy review that allows constructive new norms to appear. As we teach people to make sound ethical decisions, focused on our mission and shared values, we will grow stronger, more adaptive organizations with subordinates who are more capable of thinking through unique future problems.

---

*A broadly stated ethical framework is important in terms of professional identity, helping to define who we are as a profession.*

---

### ON BECOMING “BETTER” PROFESSIONALS

A broadly stated ethical framework is important in terms of professional identity, helping to define who we are as a profession. A code of ethics should provide an integrated view of the practitioner’s daily work, to include the nature of the client relationship, the standards of practice, and professional relationships among practitioners. A holistic view of intelligence ethics facilitates a deeper understanding of that identity and our obligations to our policy clients, subordinates, and fellow practitioners. Such a view enhances collaboration and team learning. It may be that an intelligence agency can never “be” a learning organization, but we can practice the disciplines of learning and thereby become better professionals. Our duty to the American people and our policy clients demands no less than excellence in all that we do.

[Author’s Note: The opinions expressed in this article are the author’s personal ones and do not imply endorsement by the National Intelligence University or the Defense Intelligence Agency.]

#### NOTES

<sup>1</sup> Glenn Kessler, “James Clapper’s ‘least untruthful’ statement to the Senate,” *The Washington Post*, [http://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459\\_blog.html](http://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html) (accessed 23 July 2014). Director Clapper, on the other hand, takes exception to the characterization of his admittedly erroneous answer. See DNI Letter of Senator Dianne Feinstein, 21 June 2013, URL: <http://www.dni.gov/files/documents/2013-06-21%20DNI%20Ltr%20to%20Sen.%20Feinstein.pdf> (accessed 28 November 2014); Robert S. Litt, letter to *The New York Times* editor, 3 January 2014, URL: <http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/996-letter-to-the-new-york-times-editor-from-odni-general-counsel-robert-litt> (accessed 28 November 2014); and interview with Alexander Joel, ODNI Civil Liberties Protection Officer, Steptoe Cyberlaw Podcast, 23 April 2014 (starting at 37 minutes), Lawfare Blog, URL: <http://www.lawfareblog.com/2014/04/steptoe-cyberlaw-podcast-episode-16-an-interview-with-alex-joel/> (accessed 28 November 2014). Clearly, the DNI’s comments cannot be fairly construed as a “lie.” Moreover, the DNI set an important ethical precedent for intelligence practitioners with his prompt and public clarification.

<sup>2</sup> Jan Goldman, *Ethics of Spying: A Reader for the Intelligence Professional* (Lanham, MD: Scarecrow Press, 2006), xiii.

<sup>3</sup> Jan Goldman, “Ethics of Spying,” *Defense Intelligence Journal*, vol. 14, no. 2 (2005): 48.

<sup>4</sup> *The Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), 50 U.S.C. ch. 15 § 401 et seq.

<sup>5</sup> Office of the Director of National Intelligence, “The U.S. Intelligence Community’s Five Year Strategic Human Capital Plan: An Annex to the U.S. National Intelligence Strategy,” 22 June 2006 (Washington, DC: ODNI, 2006), 28. See also Dr. Albert C. Pierce, “The Value of an Ethos for Intelligence Professionals,” remarks made at the Annual Meeting of the International Studies Association, Chicago, IL, 2 March 2007.

<sup>6</sup> Christopher E. Bailey, “The Intelligence Community Ethos: A Closely Regulated Profession,” *International Journal of Intelligence Ethics*, vol. 3, no. 2 (2012): 54-76.

<sup>7</sup> ICS 610-1, “Core Qualification Standard for Senior Civilian Officers in the Intelligence Community” (Washington, DC: ODNI, 22 February 2010).

<sup>8</sup> ICD 660, “Intelligence Community Civilian Joint Duty Program” (Washington, DC: ODNI, 11 February 2013).

<sup>9</sup> ODNI, “Principles of Professional Ethics for the Intelligence Community,” URL: <http://www.dni.gov/index.php/intelligence-community/principles-of-professional-ethics> (accessed 21 July 2014). This set of principles has also been incorporated in the 2014 *National Intelligence Strategy* that was released on 8 August 2014.

<sup>10</sup> James R. Clapper, Director of National Intelligence, remarks delivered at the AFCEA/INSA National Security and Intelligence Summit, 18 September 2014, URL: <http://www.dni.gov/index.php/newsroom/speeches-and-interviews/202-speeches-interviews-2014/1115-remarks-as-delivered-by-the-honorable-james-r-clapper-director-of-national-intelligence-afcea-insa-national-security-and-intelligence-summit> (accessed 28 November 2014).

<sup>11</sup> Senior officers have experienced a wide range of problems over the past ten years, much of which could be considered as violations of the general ethical rules binding upon all executive branch employees that are promulgated by the Office of Government Ethics. In 2012 General William “Kip” Ward was retired at reduced rank for misconduct involving lavish travel and unauthorized expenses; in November 2012 General David Petraeus was forced to step down as the CIA Director after his relationship with Paula Broadwell became public knowledge; in 2010 General Stanley McChrystal was forced to retire after inappropriate comments by his staff regarding the Vice President and others were published in a *Rolling Stone* article; in 2013 Lieutenant General David Huntoon retired amid claims that he had subordinates perform personal tasks for him; in

2012 Major General Susan Mashiko was implicated in a whistleblower/reprisal situation, along with questions about her use of an official vehicle, while at the National Reconnaissance Office; and in 2014 Brigadier General Jeffrey Sinclair was court-martialed for rape, but admitted to adultery with a subordinate. One writer claims that the U.S. Navy has an integrity problem in the ranks of its commanding officers, as demonstrated by a wide range of dismissals over the past 15 years. Captain Mark F. Light, "The Navy's Moral Compass: Commanding Officers and Personal Misconduct," *Naval War College Review* 65, no. 3 (Summer 2012): 136-152. See also Dean C. Ludwig and Clinton O. Longenecker, "The Bathsheba Syndrome: The Ethical Failure of Successful Leaders," *Journal of Business Ethics* 12 (1993): 265-273; Ludwig provides an interesting perspective on why senior leaders experience certain ethical problems.

<sup>12</sup> See, for example, the *Ethics in Government Act of 1978* (Pub. L. 95-521, as amended); 5 CFR Ch. XVI (1-1-11 Edition), § 2638.201 and *The Hatch Act*, 5 U.S.C. § 7323 et seq. See also ICD 119, "Media Contacts," or ICD 120, "IC Whistleblower Protection," (Washington, DC: ODNI, 20 March 2014).

<sup>13</sup> Samuel Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (Boston, MA: Belknap Press, 1981). See also Colonel Matthew Moten, "Who Is a Member of the Military Profession?" *Joint Force Quarterly* 62 (3d Quarter 2011): 14-17, for alternative views by sociologist James Burk and historian Allan Millett on defining a "profession."

<sup>14</sup> Intelligence practitioners cannot divorce themselves from politics; all decisions have domestic and international context that cannot be ignored. What we cannot do is inject ourselves into the policy client's business—partisan politics and choices.

<sup>15</sup> This standard of care can be defined as the degree of watchfulness, attention, caution, and prudence that a reasonable person would exercise in similar circumstances. If a person's actions do not meet this standard of care, then his/her acts fail to meet the duty of care which all practitioners have toward others and that person may be liable for "malpractice." Here, the DNI principles create an expectation (a goal) of performance at an excellence level, but without clarifying a standard of care.

<sup>16</sup> Paul D. Miller, "Lessons for Intelligence Support to Policymaking during Crises," *Studies in Intelligence* 54, no. 2 (June 2010): 1-8, 3.

<sup>17</sup> Robert Jervis, "Why Intelligence and Policymakers Clash," *Political Science Quarterly* 125, no. 2 (2010): 185-204. See also Jack Davis, "Intelligence Analysts and Policy-Makers: Benefits and Dangers of Tensions in the Relationship," *Intelligence and National Security* 21 (December 2006): 999-1021. Mark Lowenthal, former Vice Chairman of the National Intelligence Council, has also characterized the unequal relationship between the policymaker and the intelligence practitioner as a semi-permeable membrane, with the principal having greater rights in the relationship and able to cross over into the intelligence sphere. Mark Lowenthal, *Intelligence: From Secrets to Policy*, 6<sup>th</sup> ed. (Thousand Oaks, CA: CG Press, 2014), 6. See also James A. Barry and others, "Bridging the Intelligence-Policy Divide," *Studies in Intelligence* 37, no 3 (1994): 1-8.

<sup>18</sup> The DNI has a statutory obligation to act as an "advisor" to the President and the National Security Council. See 50 U.S.C.

§403 (b) (2). In a sense, the DNI's relationship to the President is analogous to an attorney-client relationship in which the attorney advises the client, but the client makes ultimate decisions about strategic issues such as whether to settle a case or proceed to trial. Moreover, even if the attorney disagrees about the client's objectives, the attorney has an obligation to argue the client's case, especially if it involves a good faith argument involving "an extension, modification or reversal" of existing law. Nonetheless, it is unethical (and usually illegal) for an attorney to assist a client in pursuing illegal activities. This view of the intelligence practitioner, as a person with heightened professional obligations, is also consistent with the Oath of Office taken by federal employees under 5 U.S.C. 3331. The Oath also clarifies that it is the President and other policymakers, in their official capacity under the U.S. Constitution, who constitute our "client."

<sup>19</sup> Robert M. Gates, "Guarding Against Politicization: A Message to Analysts," in *Ethics of Spying: A Reader for the Intelligence Professional*, edited by Jan Goldman (Lanham, MD: Scarecrow Press, 2006), 171-184.

<sup>20</sup> Josh Kerbel and Anthony Olcott, "Synthesizing with Clients, Not Analyzing for Customers," *Studies in Intelligence*, vol. 54, no. 4 (December 2010).

<sup>21</sup> Kerbel and Olcott, "Synthesizing with Clients," 17.

<sup>22</sup> Kerbel and Olcott, "Synthesizing with Clients," 18-19 (emphasis in original).

<sup>23</sup> See, for example, *The Inspector General Act of 1978*, 5 U.S.C. App. 3; *The Military Whistleblower Protection Act*, 10 U.S.C. § 1034 (protecting members of the Armed Forces who make certain communications with Congress); *The Intelligence Community Whistleblower Protection Act*, 5 U.S.C. App § 8H (protecting certain communications made by employees of the Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and the National Security Agency with Congress); and *The Notification and Federal Employee Anti-discrimination and Retaliation* (No FEAR) Act, 5 U.S.C. 2301.

<sup>24</sup> Moten, "Who Is a Member of the Military Profession?" 17.

<sup>25</sup> Peter M. Senge, "The Leader's New Work: Building Learning Organizations," *Sloan Management Review* (Fall 1990): 11 (emphasis in original). Senge also argues that when we speak of a learning organization we are not describing external phenomena, but are rather articulating a view that involves us as observers as much as it involves the observed in the common system. He also contends that learning organizations are built by communities of servant leaders. See also Daniel H. Kim, "The Link between Individual and Organizational Learning," *Sloan Management Review* (Fall 1993): 37-50.

<sup>26</sup> Fred Kofman and Peter M. Senge, "Communities of Commitment: The Heart of Learning Organizations," *Organizational Dynamics* 22, Issue 2 (Autumn 1993): 5-23, 18. See generally Robert K. Greenleaf, *Servant Leadership: A Journey into the Nature of Legitimate Power and Greatness* (Mahwah, NJ: Paulist Press, 2002).

<sup>27</sup> Edgar H. Schein, "How Can Organizations Learn Faster? The Challenge of Entering the Green Room," *Sloan Management Review* (Winter 1993): 85-92.

<sup>28</sup> David A. Thomas and Robin J. Ely, "Making Differences Matter: A New Paradigm for Managing Diversity," *Harvard Business Review* 74, no. 5 (September-October 1996): 79-90.



<sup>29</sup> Thomas and Ely, "Making Differences Matter," 6 (emphasis in original).

<sup>30</sup> Kofman and Senge, "Communities of Commitment: The Heart of Learning Organizations."

<sup>31</sup> Homer, *The Odyssey*, translated by Robert Fagles and Bernard Knox (New York: Penguin Books, 1996), 100 (lines 250-254).

<sup>32</sup> J.M. McConnell, "Intelligence Community Core Values" (Washington, DC: Director of National Intelligence, 7 August 2007).

<sup>33</sup> A certain level of "emotional intelligence" is very useful here, especially in terms of building trust in organizations. See also Daniel Goleman, *Primal Leadership: Learning to Lead with Emotional Intelligence* (Boston, MA: Harvard Business School, 2002), and Stephen M.R. Covey, *The Speed of Trust: The One Thing That Changes Everything* (New York: Free Press, 2006).

<sup>34</sup> See Dr. Richard Paul and Dr. Linda Elder, *Understanding the Foundations of Ethical Reasoning* (Sebastopol, CA: The Foundation for Critical Thinking). The book *Fair Play: The Moral Dilemmas of Spying*, by James M. Olson, a former CIA officer (Washington, DC: Potomac Books, 2006), offers useful operational vignettes that are followed by commentary from different professional, academic, and religious perspectives. The fictional works of John LeCarre and Graham Greene also provide a useful teaching method for understanding some of the unique moral/ethical operational challenges faced by intelligence

practitioners. See also Frederick P. Hitz, *The Great Game: The Myths and Reality of Espionage* (New York: Vintage Books, 2005).

<sup>35</sup> Kent Pekel, "The Need for Improvement: Integrity, Ethics, and the CIA," *Studies in Intelligence* 41, no. 5 (Spring 1998): 48, URL: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol41no5/pdf/v41i5a05p.pdf> (accessed 15 August 2014).

*LTC (USAR, Ret) Christopher E. Bailey is a faculty member at the National Intelligence University specializing in national security law, processes, intelligence ethics, and strategy. He is a 2008 graduate of the U.S. Army War College and has an LLM degree in National Security and U.S. Foreign Relations Law from the George Washington University Law School. He is licensed to practice law in California and the District of Columbia, and is a member of the American Bar Association. Chris is a frequent contributor to AIJ and volunteered to co-edit this particular issue of the Journal dealing with ethics and leadership.*

The advertisement for SOSI features a dark background with a large, stylized globe in the center. The globe is surrounded by concentric circles and lines, suggesting a global network or technology. The text "No Challenge is Too Tough" is prominently displayed in a large, bold, sans-serif font. Below this, the text "We have provided innovative logistics and intelligence solutions to customers around the world since 1989." is written in a smaller font. The SOSI logo is in the top left corner. The bottom of the advertisement features the text "CHALLENGE ACCEPTED" in a large, bold, sans-serif font. The website "www.sosi.com" is listed at the bottom left.

**sosi**

# No Challenge is Too Tough

We have provided innovative logistics and intelligence solutions to customers around the world since 1989.

**INTELLIGENCE SOLUTIONS**

- Intelligence Analytics and Training
- Information Technology and Systems Engineering
- Language and Cultural Analysis

**MISSION SOLUTIONS**

- Base Operations Support
- Engineering, Procurement and Construction
- Operations and Maintenance
- Security Assessment and Training

[www.sosi.com](http://www.sosi.com)

## CHALLENGE ACCEPTED



---

# The Big Brother Fear: Four Perspectives on Surveillance

by Dumitrina Galantonu

---

## INTRODUCTION: THE NEED FOR FRESH PERSPECTIVES

**T**he issue of mass government surveillance, especially in an increasingly interconnected electronic world, has captured the imagination of many people around the world, often resulting in increased fear and anxiety about the possible use and misuse of that collected information. Why do people react the way they do when it comes to the alleged tension between security and civil liberties? Is there a better way to understand this “tension”? This article addresses the issue of surveillance from four different perspectives. The first is a psychological perspective on the power of fear over a person’s mind. The second focuses on freedom as an understood necessity from a philosophical perspective. The third is a sociological perspective regarding the role of public debate in shaping public perceptions over the surveillance topic. A society as a whole must be educated or trained to overcome the collective fears through correct and sincere mass media communication. Last, but not least, I will discuss a logical perspective over the effect of technological development in an interconnected world.

The main focus of this article is on a person’s belief system, mindsets, fears, and anxieties. As a consequence, the article is not about choosing “the smallest evil,” but rather about understanding why human beings react so negatively to things that were not created with the purpose of diminishing their civil liberties or invading their privacy. How exactly are one’s privacy interests or civil liberties affected by mass surveillance in an open, interconnected, and technological world?

I suggest that strong negative reaction against these practices comes largely from fear of the abuse of power on behalf of government authorities. Moreover, it is this initial fear which shapes the whole belief system about privacy, surveillance, security, and necessity. The same fear makes the debate about mass surveillance more of an emotional approach about public perceptions, instead of a rational presentation about implications of “Big Data” and surveillance. People perceive these practices as threats because this is part of their underlying belief system, not

necessarily because there are strong arguments to sustain that fear. As an example, citizens do not usually have a strong negative reaction against the private sector gathering data (e.g., Amazon, e-Bay, and Facebook), but they do have a completely different reaction toward surveillance when it occurs on behalf of the government for reasons of national security.

---

*Citizens do not usually have a strong negative reaction against the private sector gathering data (e.g., Amazon, e-Bay, and Facebook), but they do have a completely different reaction toward surveillance when it occurs on behalf of the government for reasons of national security.*

---

Consequently, the question is why do people perceive the action of a government for security reasons with greater anxiety than they perceive a similar gathering of data from the private sector? Are economic interests more important than national security interests? Or are economic interests subsumed as part of our national security interests, so that the sharing of data between private and government entities can be considered normal? If these are logical assumptions, why does the fear of being surveilled persist? When one is connected automatically on Facebook with her former maiden name or is offered the chance to buy a tie that matches the suit he has just bought, is that scary? The first reaction is one of surprise and amusement, but not anger. Now if one has the same situation, but involving a government agency that processes the data about one’s Facebook profile or bank account payments, why is the reaction so different? We are surveilled, watched, and possibly affected in our daily lives because something or somebody has an invisible eye on us. In my view, the root of the problem is the ancestral fear of being revealed as you are by somebody who might hurt you. Again, I stress it is fear that dictates this reaction of rejection.

Human fear is the essential limiting factor in the surveillance debate. However, limits can be overcome. For example, the proliferation of technology in our daily lives has made possible things that were unthinkable years ago. As Patrick Meier writes in *Digital Humanitarians*, Big Data, including social media networks, form “a new nervous system in human history.”<sup>1</sup> This “new nervous system” is based on information gathering and sharing, and evolves more quickly than any other nervous system in life’s evolution. In these conditions, the way technology changes the world and how security agencies prepare for this is probably more important than an endless debate about how ethical or safe it is to use Big Data sources.

### **MINDSETS AND ATTRIBUTION THEORY: A PSYCHOLOGICAL PERSPECTIVE ON SURVEILLANCE**

**S**urveillance is defined as “the monitoring of the behavior, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them.”<sup>2</sup> From such a definition one might emphasize the positive approach: the monitoring of behavior in order to protect people. Or one might emphasize the negative aspect: monitoring the activities for hidden purposes, such as influencing, manipulating, conducting blackmail against, and taking advantage of an adversary.

---

*Attribution theory focuses on the judgments that people make about the cause of an event or a behavior; this theory helps us understand the crucial role that judgment plays in the surveillance debate and the liberty vs. security dilemma.*

---

The way people perceive something, as being either positive or negative, depends on the often-unconscious judgments made by our minds. This can cause us to “attribute” things to an external reality that may or may not be there. Attribution theory focuses on the judgments that people make about the cause of an event or a behavior; this theory helps us understand the crucial role that judgment plays in the surveillance debate and the liberty vs. security dilemma.

I suggest that we commit a fundamental “attribution error” when we favor more security requirements, as opposed to lesser civil liberties. With such an approach, we overlook the

power and the advent of technology that has already created an extremely open society, meaning more transparent and speedy, where almost everything and everyone is connected.

An open society, as French philosopher Henri Bergson and later Karl Popper conceived it, is marked by a critical attitude toward tradition.<sup>3</sup> That means the “government is expected to be responsive and tolerant, and political mechanisms are said to be transparent and flexible.” Popper defined open society as being one in which individuals are confronted with personal choices as opposed to a collectivist society. That has been often understood as being more in terms of political freedoms and human rights, and less the idea that an open society means the individuals are confronted with their personal decisions, as well. In other words, people are accountable for their actions, anytime, and that is not necessarily because somebody watches them or forces them to take responsibility for their own deeds.

---

*If we are not free from fear, we cannot actually gain full cognitive capacity on any given topic or issue.*

---

An open society “would keep no secrets from itself in the public sense, as all are trusted with the knowledge of all.”<sup>4</sup> In the meantime, an open society means an increase in personal responsibility for moral choices. I would suggest that, in changing the mindset from fear to trust, we might be surprised by having both liberty and security, and something more: the knowledge about what is necessary and why. In this regard, it is more important to set correctly the basic belief system of the citizens.

There has been extensive research, as well as anecdotal evidence, that anxiety affects the human thinking skills: “It can be an adaptive healthy response or a debilitating one. In the latter case, one may lose a large measure of ability to think, act, and perform. Anxiety is manifested in at least three ways: in a person’s thoughts (cognitively), in a person’s actions (behaviorally), and in physiological reactions.”<sup>5</sup> Thus, if we are not free from fear, we cannot actually gain full cognitive capacity on any given topic or issue.

As it looks now, the belief systems that shape the public perceptions on surveillance are also shaped by the fear of losing privacy. It is, first of all, the fear of abuse of power and totalitarianism. History shows us that absolute power corrupts, but mankind should switch the emphasis from the past toward the future: in a very technological and interconnected world, facts, events, and behaviors are

easier to discover, sometimes due to surprising interconnections and not as a result of surveillance. The idea of isolation and secrecy might appear obsolete from many points of view. We could see the Internet with its amazing capacity of connection as the technological communion of all the pieces of information, based on communication and sharing. Thus, we can understand that surveillance is a result of the need to connect and integrate all pieces of information, as we move faster and faster with the technology.

### **LIBERTY AS FREE NECESSITY: A PHILOSOPHICAL PERSPECTIVE ON SURVEILLANCE**

**T**he Dutch philosopher Baruch Spinoza claimed that if you understand your necessity you are free. Yet, according to common sense, these two terms—freedom and necessity—are usually understood as being in opposition. Spinoza places freedom “not in free decision, but in free necessity.”<sup>6</sup> In order to exemplify his thinking, he gives the following example:

A stone receives from the impulsion of an external cause a fixed quantity of motion whereby it will necessarily continue to move when the impulsion of the external cause has ceased... Furthermore, conceive, if you please, that while continuing in motion the stone thinks, and knows that it is endeavoring, as far as in it lies, to continue in motion. Now this stone, since it is conscious only of its endeavour and is not at all indifferent, will surely think it is completely free, and that it continues in motion for no other reason than that it so wishes. This, then, is that human freedom which all men boast of possessing, and which consists solely in this, that men are conscious of their desire and unaware of the causes by which they are determined. In the same way a baby thinks that it freely desires milk, an angry child revenge, and a coward flight. So, too, the delirious, the loquacious, and many others of this kind believe that they act from their free decision, and not that they are carried away by impulse. Since this preconception is innate in all men, they cannot so easily be rid of it.<sup>7</sup>

Spinoza’s analysis of liberty and freedom adds an important dimension to the bipolar liberty-security concept: the concepts of necessity and of understanding. Hence, the complete chain of analysis should be liberty—understanding—necessity—security. A person is freer if one understands the necessity of security than if one struggles for more civil liberties.

For Spinoza, power is the knowledge of necessity. He explains that powerful—meaning virtuous—persons act because they understand why they must act. Knowledge and the understanding of adequate ideas make a person free. According to Spinoza, in a society where all persons live by the direction of reason, there will be no need for political authority to restrict people’s behaviors. Unfortunately, people do not always live and act under the guidance of rationality. This actually creates the necessity of a state as the guarantor of freedom and that it is necessary to ensure, through the threat of force (i.e., the police power of the state), that individuals are protected from other individuals. The state can then become the rational agent that checks and balances the irrational power of the population.<sup>8</sup>

Spinoza argues that the emotions might be the most serious threat to a person’s freedom. A man should endeavor to free himself from the passions and emotions that affect his ability to reason. It is the same case with an emotional reaction toward what the government might do, for hidden reasons.

Edward Younkins argues that, as we acquire a greater understanding of the causes acting on us, actually our freedom increases. In a similar manner, Paul Kashap offers that “men are not born free, they attain freedom.”<sup>9</sup> This means that: “Man is naturally subject to passions; he follows the common order of nature, adjusting himself and his self-interests to the requirements of his environment.”<sup>10</sup> In this case, one requirement of his environment might be security. If he understands how his security can be achieved, he has greater chances of becoming free than if he lives in continuing fear of losing his freedom. This analysis underscores the same basic idea: man becomes free through understanding, knowledge, and truth. Thus, it is possible to conclude that citizens would be more free if they knew the truth about mass surveillance capabilities, and the necessity for them, than if they remained in a seemingly endless debate with half-true statements about what the state is allowed to do or already does.

### **LIBERTY-SECURITY PUBLIC DEBATE: A SOCIOLOGICAL PERSPECTIVE**

**B**enjamin Franklin is often quoted as saying: “They that can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.” His words capture the perennial dilemma involving the “trade-off” between privacy and national security. Many times, when following these types of dichotomy, we end up in other linguistic and logic traps, trying to choose between unsatisfactory—apparent either/or—

alternatives. Instead, it would be better for intelligence professionals and for the general public to understand where this dilemma comes from. This could lead to a deeper, richer understanding about the ongoing public debate on acceptable intelligence practices.

One should understand that our beliefs and our perceptions are mostly shaped by the *fear* of losing privacy, with no clear evidence about actual abuses of power. In other words, as citizens we have to deal openly with the fact that we have a great fear of being surveilled, while we do not necessarily know what that means.

I would say that privacy vs. national security is more an issue of public perception than it is an issue about losing fundamental liberties. In terms of civil liberties, the collection of Big Data does not really affect people. In terms of personal freedom and privacy, the debate is more sensitive, but still not the scary Orwellian scenario of 1984. Even if we all agree that data collection has implications for everybody, in a truly open and transparent society where everybody is accountable for their deeds, that does not make any of us necessarily a target of the abuse of power. We all give the same kind of information and receive the same kind of treatment.

I do not suggest that one should agree with whatever a government might suggest in the name of security. Instead, I feel that facing openly our fears as citizens might be a better way to get freedom (one accepted view of freedom is to be free from our own fears), based on knowledge, responsibility, and long-lasting security.

Two international law documents, the *International Covenant on Civil and Political Rights* (ICCPR) and the *Universal Declaration of Human Rights* (UDHR), provide a useful starting point for what we mean by civil liberties. The ICCPR, Article 9, provides that: "Everyone has the right to liberty and security of person."<sup>11</sup> Here, it is apparent that the concepts involving liberty and security are not necessarily in opposition, but can be complementary. The Covenant also says that, "in accordance with the Universal Declaration of Human Rights, the ideal of free human beings enjoying civil and political freedom and freedom from fear and want can only be achieved if conditions are created whereby everyone may enjoy his civil and political rights, as well as his economic, social and cultural rights."<sup>12</sup> In other words, "the freedom from fear" is critical, likely as critical as having the actual freedoms.

Does one really "lose" civil liberties when he knows about, accepts, and probably agrees with mass surveillance? What exactly is behind this fear? Is it a specific mindset, a system of beliefs that makes us

perceive mass surveillance as an attack on our civil liberties? The public debate on this topic is usually biased by emotional reactions that result from negative public perceptions about surveillance. Frankly, people fear that somebody will abuse power. The negative reaction is even bigger, as long as people actually face more anxiety than fear, because anxiety creates a worse perception. Why? The difference is that fear has a clear object, while anxiety does not have a clear enemy. I consider this to be the case even with the surveillance fears: it is not somebody or something that one can identify. Instead, in the public perception, it is a presence that can take any form, anytime, and anywhere. In this way, people can attain high levels of anxiety. Unfortunately, besides the negative emotions that one feels when facing high levels of anxiety, the value that is often the most affected will be his/her mental capacity to discern between good and evil, harmful or inoffensive.

### **"BIG DATA" AND THE PRICE OF TECHNOLOGY: A LOGICAL PERSPECTIVE ON SURVEILLANCE**

**B**ig Data" is constantly generated by everything around us: from how people are guided to potential purchases as they shop online to political campaigns. E-commerce retailers at Amazon or E-Bay can use accumulated data on past Internet browsing histories to send targeted and personal advertising to specific customers. In fact, retailers actually build algorithms for applications such as the "You Might Like" feature. Every digital process and social media exchange produces "Big Data." Systems, sensors, and mobile devices transmit it every day, some wanted and some unwanted. Yet, no one seems bothered about their devices gathering and offering data. "Every day, we create 2.5 quintillion bytes of data—so much that 90 percent of the data in the world today has been created in the last two years alone," according to IBM.<sup>13</sup>

What also should one know about Big Data? For example, the Big Data that results from the U.S. National Security Agency (NSA) surveillance program is not necessarily a good in and of itself, because Big Data comes with a huge amount of work. Data management can be a real burden, especially when most of the collected data is unneeded and unwanted. Most people, and most communications, are not involved in government spying; it is the narrower things, like terrorism or other state secrets, that interest government organizations such as NSA.

Thus, one might ask that, if the collection of data is not as useful as it is supposed to be, why would a government agency collect it? The simple answer to this question involves the way the technology has shaped the modern



world: it is just as easy and natural to collect any kind of information that might be helpful in answering mission-critical requirements. Thus, it is already known that the huge amounts of information collected by the Intelligence Community require continuous transformation and adaption in the way that information is processed, organized, combined, and presented. In fact, the Intelligence Community faces the data challenges of the “four Vs” of Big Data: variety, volume, velocity, and veracity.<sup>14</sup> This then leads to the question about how Big Data is organized and managed to find the golden nuggets of intelligence.

In that way, the problem really is not the *collection* of information, some of which might involve sensitive personal data, but rather *the safeguards to prevent its use by unauthorized persons or for unauthorized reasons*. Generally speaking, when talking about Big Data as a result of surveillance, the problem is not the volume, which is expected to increase, but the sensitive aspect is who might have access to that data and what they might do with it: “Big Data itself is ethically neutral; it is the actual use of Big Data that raises ethical questions.”<sup>15</sup>

The public needs the information to understand why surveillance is a public good; the public needs to know that this surveillance does not mean it will lose its privacy. In the end, the main purpose of this is to keep an eye on those who want to harm us or do bad things. On the other hand, this openness of mind should not be taken to the other extreme: of giving sensitive data, such as credit card numbers or bank accounts, to anybody who might ask for this type of information.

## TOWARD A BROADER UNDERSTANDING

This article seeks to shed light on the ancient but still debated trade-off between the concepts of security and liberty, given the technological proliferation that makes surveillance not only possible but also necessary. From the words of Benjamin Franklin to the modern International Covenant on Civil and Political Rights, we have every reason to believe that liberty and security are important rights and there is no excuse to lose any part of either.

The novelty of this article resides in the argument that we shift our attitudes when it comes to mass surveillance. We should change the emphasis from fear and anxiety, meaning negative perceptions, to an increased knowledge about the topic for every citizen. The philosophical approach of Baruch Spinoza, which considered liberty in terms of “free necessity,” gave us one good reason for adjusting our understanding of the “trade-off.” In addition, attribution theory (that is concerned with

people’s judgment about the cause of an event or a behavior) supports the need for a shift in how we view surveillance. What if, instead of automatically attributing surveillance to the loss of something, we focused more on understanding the necessity of a certain action or the outcomes that come with gathering such an amount of information? *Thus, the actual problem is not the mass surveillance itself, but the perceptions that people have about this practice*. We have to target the belief system when it comes to understanding the requirements of security in a globalized, interconnected, and technological environment.

No one can guarantee that the abuse of power might not happen one day. Nevertheless, equally nobody can fear that the possibility of accessing information about one’s private life, for strong reasons, means automatically the loss of civil liberties for the whole of humankind.

My idea is that we should understand this ongoing debate about security and liberty is actually a debate about a mindset focused on the fear of losing something: privacy. Liberty and security are not quantifiable goods. Instead, they refer to emotions and attitudes, like trust and fear.

I support neither a police state nor totalitarianism. Instead, I support a shift in the emphasis of the debate from a complete rejection of mass surveillance to understanding what that means exactly and for what it can actually be used. I give neither an uncritical “YES” to mass surveillance nor necessarily to anything else that the government might suggest in the name of security. I support a more courageous and open-minded attitude toward these practices. We must avoid a categorical “NO,” and overcome the fear and the anxiety that many people feel, often unconsciously. Furthermore, since science and scientific thought have appeared, man has usually found that the most successful way to treat fear is through increased knowledge that is the right information, processed in the right way.

[Author’s Note: The opinions expressed in this article are the author’s personal ones and do not imply endorsement by either the Romanian National Intelligence Academy or the U.S. National Defense University.]

## NOTES

<sup>1</sup> Patrick Meier, *Digital Humanitarians*, New York: CRC Press, 2015, p. 29.

<sup>2</sup> “Surveillance,” Wikipedia, <https://en.wikipedia.org/wiki/Surveillance> (accessed November 1, 2015).

<sup>3</sup> “Open Society,” Wikipedia, [https://en.wikipedia.org/wiki/Open\\_society](https://en.wikipedia.org/wiki/Open_society) (accessed October 6, 2015).

<sup>4</sup> Ibid.

<sup>5</sup> Carissa Kelvins, *Fear and Anxiety*, <http://www.csun.edu/~vcpsy00h/students/fear.htm> (accessed October 6, 2015).

<sup>6</sup> Baruch Spinoza, *Complete Works*, <http://www2.dsu.nodak.edu/users/dmeier/31458292-Spinoza-Complete-Works.pdf> (accessed October 6, 2015).

<sup>7</sup> Ibid., 908.

<sup>8</sup> Edward Younkins, *Spinoza on Freedom, Ethics and Politics*, <http://www.quebecoislibre.org/06/060507-2.htm> (accessed October 6, 2015).

<sup>9</sup> Paul Kashap, *Spinoza and the Moral Freedom*, <https://books.google.com/books?id=UfZ3NiFkhR8C&pg=PA164&lpg=PA164&dq=Men+are+not+born+free,+they+attain+freedom&source=bl&ots=mFKyQDAg3b&sig=BxNdeCK52BuRWpAHOwZKxvlnk&hl=en&sa=X&ved=0CB4Q6AEwAGoVChMI0NSzuH2awMhIk-Ch0RvQh0#v=onepage&q=Men%20are%20not%20born%20free%2C%20they%20attain%20freedom&f=false>, p. 165 (accessed October 6, 2015).

<sup>10</sup> Ibid.

<sup>11</sup> The International Covenant on Civil and Political Rights (ICCPR), adopted and opened for signature, ratification and accession by General Assembly Resolution 2200A (XXI) of December 16, 1966, entry into force on March 23, 1976.

<sup>12</sup> Ibid., citing the UN General Assembly, *Universal Declaration of Human Rights*, December 10, 1948, 217 A

(III), available at: <http://www.refworld.org/docid/3ae6b3712c.html> (accessed October 5, 2015).

<sup>13</sup> What Is Big Data? <http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html> (accessed October 6, 2015).

<sup>14</sup> Ibid., 25.

<sup>15</sup> Karl F. Schneider, David S. Lyle, and Francis X. Murphy, "Framing the Big Data Ethics Debate for the Military," *Joint Force Quarterly* 16 (2<sup>nd</sup> Quarter, 2015),

*Dumitrina Galantonu earned bachelor's and master's degrees from Alexandru Ioan Cuza University in Iasi, Romania. She has extensive experience as a journalist working on Romanian national security issues. She has been a PhD candidate at the National Intelligence Academy Mihai Viteazul in Bucharest since 2010. In 2014-15 she was a Fulbright Scholar at the National Defense University, Fort Lesley J. McNair, in Washington, DC, with her research focus on intelligence ethics, and is now back in Bucharest completing her doctorate.*



**THE VALUE OF  
CHANGING OPEN  
SOURCE DATA  
INTO ACTIONABLE  
INTELLIGENCE.**

**THE VALUE OF PERFORMANCE.**

**NORTHROP GRUMMAN**

[www.northropgrumman.com](http://www.northropgrumman.com)

© 2014 Northrop Grumman Corporation

---

# Hegelian Dialectics as a Source of Inspiration for the Intelligence Community

by Dr. Pelle de Meij

---

## OVERVIEW

This article analyzes how the ideas of the German philosopher Georg Hegel, with origins stemming from ancient Chinese and Greek society, could be used to find an answer to the question of how the Intelligence Community should operate and function generally in our modern Western society.



Georg Wilhelm Friedrich Hegel (1770-1831)

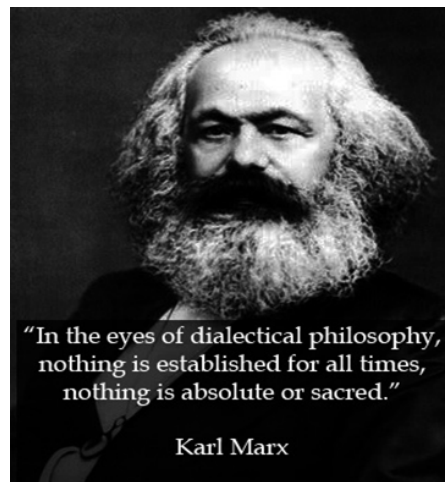
**Thesis: The Intelligence Community is the ultimate guardian of the rule of law, democracy, and human rights.**

## AN INTRODUCTION TO HEGELIAN DIALECTISM

In ancient history, thinkers sought to understand nature as a whole, and saw that everything is fluid, constantly changing, coming into being, and passing away. The distinction between the human brain as “subjective” and

nature as “objective” that has been made by the philosopher Immanuel Kant is artificial, according to Hegel and many other philosophers, because it is unreal to consider human beings as independent from nature, of which they are a part. It was only when the piecemeal method of observing nature in bits and pieces, practiced in Western thinking in the 17th and 18th centuries, made things more comprehensible that conditions became ripe for modern dialectics to make its appearance. It was the German philosopher Georg Hegel (1770-1831) who was able to sum up this picture of universal interconnection and the mutability of things in a system of logic which is the foundation of what today is called Dialectics.

The dialectical philosophy devised by Hegel underpins the entire political and social strategy of our modern Western society. Karl Marx and Friedrich Engels—who began as supporters of the philosopher Ludwig Feuerbach (1804-1872) but soon came to oppose his ideas—adhered to the Hegelian dialectic but tried to fund it on a materialist basis. According to Engels, Hegel was an idealist. To Hegel, the thoughts within the brain were not more or less abstract pictures of actual things and processes. Conversely, things and their evolution were, in the opinion of Hegel, only the realized pictures of the “Idea,” existing somewhere from eternity before the world was. This way of thinking turned everything upside down in the eyes of the founders of communism, and completely reversed the actual connection of things in the world.



Although Marx and Engels, like Hegel, favored collectivism over individualism, the approach of Hegel to “consensus-building” (compromise) and “conflict resolution” (dialogue) differs in an important way from the ideas of Marx and Engels and their theory of historical materialism. The Marxist dialectic and the Hegelian dialectic differed also in the definition of the actual forces with which the dialectic operated. For Marx and Engels the contradictory nature of our thoughts had their origin in the contradictions within human society. According to them, dialectics were a product of human labor changing the world, which could be understood only by the practical struggle to overcome these contradictions, not just in thought but also in practice.

For Hegel, ideas (in general) were the keyword. In his opinion, thoughts were not passive and independent reflections of the material world. Hegel believed that everything is constantly changing (“mutability”), which can be seen as a kind of moral relativism. The concept of change is indeed central to Hegelian dialectical theory and strategy. Some of Hegel’s (radical) young followers considered therefore the outcome of the Hegelian dialectical process shades of gray instead of black and white.<sup>1</sup>

According to Hegel, everything that is reasonable is real. In his opinion the law is the expression of this reality, which can be considered as freedom. In his State Theory, Hegel focused on the substance of life and the law. Formalism—which is often used to minimize or even suppress reasonable and legitimate criticism or protest in our contemporary society—does not fit in the Hegelian concept of the state. Therefore, it is not surprising that, according to Hegelian State Theory, the legislative and the executive are the primary state powers while the judiciary with its procedures and (procedural) fictions is secondary.

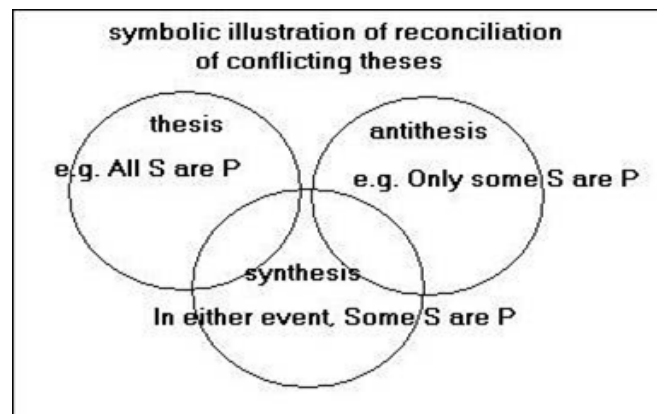
In a way, the Hegelian concept of the state corresponds with the more recent ideas of Herbert Marcuse (1898-1979), who argued that “advanced industrial society” created false needs, which integrated individuals into the existing system of production and consumption via mass media, advertising, industrial management, and contemporary modes of thought. This results, according to Marcuse, in a “one-dimensional” universe of thought and behavior, in which aptitude and ability for critical thought and oppositional behavior wither away<sup>2</sup> (cf. Herbert Marcuse, *One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society*, 1964). Beginning in 1943 Marcuse worked for the Research and Analysis Branch of the Office of Strategic Services (OSS), the precursor of the Central Intelligence Agency (CIA).

The Hegelian Formula and the role of the intelligence community in Hegel’s original intent was to devise a method to resolve disagreements and control outcomes. The Hegelian formula is typically expressed as follows: Thesis represents an idea or opinion; antithesis represents the

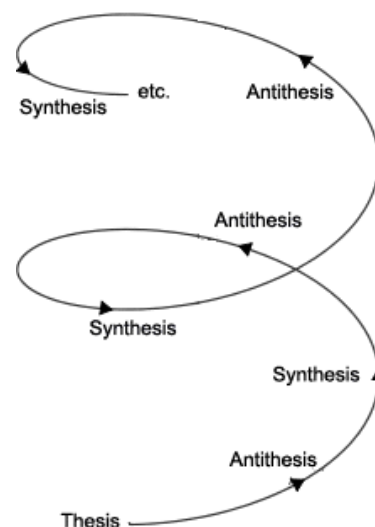
counter-opinion or opposite idea; synthesis represents the domain where thesis and antithesis intersect and overlap. In other words, dialectical synthesis can represent consensus, i.e., “compromise.” The Hegelian formula can be reflected in brief in the following way:

**THESIS+ANTITHESIS=SYNTHESIS**

**PRO+CON=CONSENSUS(COMPROMISE)**



The interesting and powerful feature of the Hegelian dialectic is that, once the circular argument has reached synthesis, a new thesis can be created and the process begins anew, incrementally and progressively moving forward toward the next predetermined outcome—a sort of dialectic helix.



Applying the Hegelian strategy can be accomplished through a process of tension and resolution, used in a



repetitive and incremental fashion. The use of tension and resolve can be an important response when a group of people is divided by conflicts. The Hegelian dialectic reduced to its simplest form could be summed up as problem, reaction, and solution, which could also be useful for intelligence work—resolving eventual conflicts by means of compromise. First of all, however, the network of intelligence services in a country should be equipped to function—in mutual cooperation—as the ultimate and proper guardian of the rule of law, democracy, and human rights. In my opinion, this could also mean that in extraordinary cases, and of course only if necessary,<sup>3</sup> one or more members of a malfunctioning judiciary or government are overruled by the Intelligence Community.

**Antithesis: Well-structured control mechanisms are needed for intelligence services.**

## PROTECTION AGAINST FAILURES OF INTELLIGENCE SERVICES

The judiciary is unable to control the Intelligence Community in a sufficient manner, because it can never investigate all relevant facts and documents for the fulfillment of that task itself. This view is expressed in the legislative history of the Netherlands' so-called Dutch Act, which consists of criminal law provisions providing for the protection of the right to privacy going back to 1971.<sup>4</sup> Nevertheless, a fundamental prerequisite for the proper functioning of intelligence services in general is that they consist of well-equipped internal and external control mechanisms. Because of their extraordinary structure and due to these control mechanisms, intelligence services can be considered as independent and impartial.

## THE INTELLIGENCE COMMUNITY AND ITS CONTROL MECHANISMS IN THE UNITED STATES

The well-known internal and external control mechanisms for the Intelligence Community in the United States can serve as an important example for many countries in the world as to how the activities of intelligence services can and should be controlled. Like other U.S. government agencies, agencies within the Intelligence Community are subject to the laws of the state (including treaty obligations), the policies of a democratic chosen head of state and, last but not least, their own internal directives. To ensure compliance with these laws, policies, and internal directives, intelligence agencies are subjected to oversight by elements within their own organizations as well as by external elements. The external elements include oversight mechanisms both in legislative and administrative bodies. Each element of the Intelligence

Community is/should be subject to the jurisdiction of an Inspector General, either within its own organization or within its parent organization.

In the United States, the CIA's Inspector General, appointed by the President and confirmed by the Senate, is responsible for investigating any alleged improprieties or program mismanagement within the CIA. The CIA Inspector General submits semi-annual reports of his activities to the two Congressional intelligence committees and must report directly to these committees under certain circumstances. The Department of Defense (DoD) also has an Inspector General created by statute who reports to the Secretary of Defense and whose jurisdiction extends to all of the intelligence elements of DoD. In addition, each such element (e.g., NSA, DIA, NRO) has its own non-statutory Inspector General, appointed by the head of the agency, who performs oversight. Non-DoD intelligence elements similarly are subject to oversight by independent Inspectors General. For example, the Bureau of Intelligence and Research at the Department of State is subject to oversight by the Department's Inspector General, and the FBI's National Security Division by the FBI Inspector General. The General Counsels of intelligence agencies also perform an oversight function, reviewing proposed and ongoing activities to ensure their compliance with law and policy.

The Intelligence Community is also subject to external oversight by the executive and legislative branches. Within the executive, the Office of Management and Budget plays a role in ensuring consistency with the President's program. Within the Congress, principal oversight responsibility rests with the two intelligence committees, but other committees occasionally become involved in an oversight role. Another important external control mechanism is the President's Intelligence Advisory Board (PIAB). The PIAB is an entity within the Executive Office of the President formed "to assess the quality, quantity, and adequacy" of intelligence collection, analysis, counterintelligence, and other activities of the Intelligence Community. The PIAB reports directly to the President, and provides recommendations for actions to improve and enhance the performance of intelligence efforts. It also examines issues raised by the President or the Director of National Intelligence (DNI) and can make recommendations directly to the DNI. The PIAB consists of not more than 16 individuals who are appointed by the President. The Intelligence Oversight Board (IOB) was made a standing committee of the PIAB in 1993 and is composed of four members of the PIAB appointed by the PIAB Chairman. The IOB conducts independent oversight investigations as required and reviews the oversight practices and procedures of the inspectors general and general counsels of the intelligence agencies.

The Office of Management and Budget (OMB) is part of the Executive Office of the President. It reviews intelligence budgets in the light of Presidential policies and priorities, clears proposed testimony, and approves draft intelligence legislation for submission to Congress. Principal oversight responsibility rests with the two intelligence committees of Congress. By law, the President must ensure that these two committees are kept “fully and currently” informed of the activities of the Intelligence Community, including any “significant anticipated intelligence activities.” Notice is also required to be provided to both committees of all covert action programs approved by the President as well as all “significant intelligence failures.”

The members of the Senate Select Committee on Intelligence (SSCI) vary from 13 to 17, with the majority party in Congress having one more member than the minority. Members of the SSCI serve 8-year terms. In addition to its role in annually authorizing appropriations for intelligence activities, the SSCI carries out oversight investigations and inquiries as required. It also handles Presidential nominations referred to the Senate for the positions of DNI, Deputy DNI, and CIA Inspector General, and reviews treaties referred to the Senate for ratification as necessary to determine the ability of the Intelligence Community to verify the provisions of the treaty under consideration. The membership of the House Permanent Select Committee on Intelligence (HPSCI) is set at 19 members and is proportional to the partisan makeup of the entire House of Representatives. Members may be appointed for terms of up to eight years. Like its Senate counterpart, the HPSCI conducts oversight investigations and inquiries in addition to processing the annual authorization of appropriations for intelligence. In addition to the intelligence committees, other Congressional committees occasionally become involved in oversight matters by virtue of their overlapping jurisdictions and responsibilities. The armed services committees of each house, for example, exercise concurrent jurisdiction over DoD intelligence activities and the judiciary committees in each house exercise concurrent jurisdiction over FBI intelligence activities.<sup>5</sup>

**Synthesis: Intelligence work is and should be of excellent quality.**

## **INTELLIGENCE WORK WITH DUE REGARD FOR VITAL INTERESTS OF SOCIETY AND FUNDAMENTAL VALUES**

**I**ntelligence services are sometimes critically considered as “a state within the state,” which makes them—apart from internal external control mechanisms—difficult to control. According to legislative history related to the former

Dutch Intelligence and Security Services Act of 1987, a good solution to this control problem can be found by focusing on the main purpose of intelligence services: the protection of the democratic legal order and the security of the state. The result of this approach should be that the purposes and working methods of the intelligence services correspond with these vital interests and fundamental values of our society.<sup>6</sup> In my opinion, the following Principles of Professional Ethics for the U.S. Intelligence Community<sup>7</sup> can be considered as important guidelines for conduct:

“As members of the intelligence profession, we conduct ourselves in accordance with certain basic principles. These principles are stated below, and reflect the standard of ethical conduct expected of all Intelligence Community personnel, regardless of individual role or agency affiliation.”

Many of these principles are also reflected in other documents that we look to for guidance, such as statements of core values and the Code of Conduct: Principles of Ethical Conduct for Government Officers and Employees; it is nonetheless important for the Intelligence Community to set forth in a single statement the fundamental ethical principles that unite us—and distinguish us—as intelligence professionals.

### **Mission**

We serve the American people, and understand that our mission requires selfless dedication to the security of our Nation.

### **Truth**

We seek the truth; speak truth to power; and obtain, analyze, and provide intelligence objectively.

### **Lawfulness**

We support and defend the Constitution, and comply with the laws of the United States, ensuring that we carry out our mission in a manner that respects privacy, civil liberties, and human rights obligations.

### **Integrity**

We demonstrate integrity in our conduct, mindful that all our actions, whether public or not, should reflect positively on the Intelligence Community at large.

### **Stewardship**

We are responsible stewards of the public trust; we use intelligence authorities and resources prudently, protect intelligence sources and methods diligently, report wrongdoing through appropriate channels, and remain accountable to ourselves, our oversight institutions, and through those institutions, ultimately to the American people.

## Excellence

We seek to improve our performance and our craft continuously, share information responsibly, collaborate with our colleagues, and demonstrate innovation and agility when meeting new challenges.

## Diversity

We embrace the diversity of our Nation, promote diversity and inclusion in our work force, and encourage diversity in our thinking.”

## THE WORKING FIELD OF INTELLIGENCE SERVICES IN GERMANY AS A TOUCHSTONE FOR QUALITY

Article 4, no. 2 of the German Federal Intelligence Agency Act<sup>8</sup> gives a detailed description of the democratic legal order that needs to be protected by the intelligence service and forms the working field of this service. The democratic legal order includes, according to this provision: (a) the right of the people to exercise the state authority in free and secret elections and through organs of the legislative, executive, and judicial authority; (b) the binding of the legislative, executive, and judicial authority to the constitutional order and the law; (c) the right to education and to exercise parliamentary opposition; (d) the removability of the government and its accountability to the representatives of the people; (e) the independence of the courts; (f) the exclusion of any violence and tyranny; and (g) the human rights specified in the constitution.

From the above-mentioned, a detailed description could be extracted regarding proper guidelines for intelligence work.

## CONCLUSION

In case of emergency, society needs to rely on its intelligence services. A fundamental prerequisite for the proper functioning of intelligence services is that they consist of well-equipped internal and external control mechanisms. The extraordinary structure of intelligence services and these control mechanisms make them—perhaps even more than the judiciary—independent and impartial. In the discussion of how intelligence services should be controlled properly, one should focus on the main purpose of these services: the protection of the democratic legal order and the security of the state. The result of this approach should be that the purposes and working methods of the intelligence services correspond with the vital interests and fundamental values of our society. The Intelligence Community should resolve eventual conflicts by means of compromise to the extent possible.

[Author’s Note: The pictures and figures in this article are derived from <http://www.therightplanet.com>. The article is

written in a personal capacity and dedicated to the Dutch General Intelligence Service (AIVD) in gratitude for its support in difficult circumstances.]

## NOTES

<sup>1</sup> Cf. Friedrich Engels, *Socialism: Utopian and Scientific*; *Ibidem*, *Dialectics of Nature*, <https://www.marxists.org/glossary/terms/d/i.htm>.

<sup>2</sup> Cf. Herbert Marcuse, *One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society*, 1964. Beginning in 1943, Marcuse worked for the Research and Analysis Branch of the Office of Strategic Services (OSS), the precursor of the Central Intelligence Agency (CIA).

<sup>3</sup> See also the website of the Dutch General Intelligence Service (AIVD) that stresses the importance of the observance of the principle of proportionality in cases where people’s privacy is at stake; <https://www.aivd.nl/onderwerpen/het-werk-van-de-aivd/inhoud/de-aivd-en-privacy>.

<sup>4</sup> Wet van 7 April 1971, Stb. 1971, 180, houdende enige strafbepalingen tot bescherming van de persoonlijke levenssfeer, Nadere Memorie van Antwoord, Kamerstukken II, 1969-1970, 9414, nr. 8, p. 3. See also: rov. 4.4.2 of Supreme Court of the Netherlands, 5 September 2006, nr. 01422/05, ECLI:NL:HR:2006:AV4122, NJ 2007, 336.

<sup>5</sup> <http://fas.org/irp/offdocs/int023.html>.

<sup>6</sup> Wet op de Inlichtingen-en Veiligheidsdiensten van 3 December 1987, Stb. 1987, 63, Memorie van Toelichting, Kamerstukken II, 1981-1982, 17363, nr. 3, p. 2; the Act of 1987 was replaced in 2002 with a new Intelligence and Security Services Act: Wet van 7 februari 2002, Stb. 2002, 148. See also rov. 4.4.1 of Supreme Court of the Netherlands, 5 September 2006, nr. 01422/05, ECLI:NL:HR:2006:AV4122, NJ 2007, 336.

<sup>7</sup> <http://www.dni.gov/index.php/intelligence-community/principles-of-professional-ethics>.

<sup>8</sup> Bundesverfassungsschutzgesetz from 20 December 1990, BGBl. I S. 2954, 2970, as last amended by Article 1 of the Law from 17 November 2015, BGBl. I S. 1938.

*Dr. Pelle de Meij is a member of the Legal Science Department of the Supreme Court of the Netherlands, with special research interest in private international law, transport/maritime law, and tax law. In 1994 he earned a master’s degree in law from the University of Utrecht following studies in Regensburg, Germany. After his law studies he participated in a Modern Greek language course at the University of Thessaloniki in Greece. He then taught contract law, private international law, and transport law for four years at the University of Groningen, in the north of the Netherlands. In 2003 he earned a doctorate in law upon finishing a dissertation on the concurrence of the international road transport treaty and European Union regulations on the jurisdiction, recognition, and enforcement of judgments in civil and commercial matters.*



---

# The Road to High-Quality Decision-Making: Understanding Cognition and the Phenomenon of Groupthink

by Troy E. Smith

---

Strategy is a plan of action designed to achieve a long-term or overall goal. To put this into perspective as it relates to decision-makers, strategy is the plan that results from a decision or series of decisions to achieve a long-term or overall goal in the context of political issues, choices, and conflict. The part of this definition that needs particular attention is “decisions.” The ability to make well-informed and rational decisions is essential for the formation of any good strategy. Poor strategy or inappropriate choice in tactics leading to flawed implementation of strategy is directly linked to the analysis on which it is derived. Development of an effective strategy requires critical analysis of a multitude of factors in order first to make assumptions about the environment and the problem from which the ends, ways, and means triangle can be constructed.<sup>1</sup> Ideally in a high-quality decision-making process, assumptions are thoroughly examined to identify the practicality of the assumptions and the impact should they be wrong.

---

*Cognitive biases are the result of subconscious mental procedures for processing information. These mental errors are consistent and predictable...*

---

In this examination all information is processed critically and devoid of internal and external biases. However, decision-making and information processing are highly dependent on attitude and the cognitive processes which are at the top of our consciousness. The human mind is influenced easily by internal and external factors leading to cognitive errors or errors in processing. The systematic deviation of what is considered to be a standard of rationality or good judgment due to intrinsic and extrinsic factors is termed “bias.” While bias can take many forms, such as cultural bias, organizational bias or bias that results from one’s own self-interest, here we focus on cognitive bias.<sup>2</sup> Cognitive biases are the result of subconscious mental procedures for processing information. These mental errors are consistent and predictable, which makes understanding them and developing mitigation techniques potentially easier. This

article looks at the cognitive errors or biases, which result from the use of heuristics and groupthink, effectively looking at how we process information, how we represent problems, and the effects of group dynamics on the cognitive process.

Cognitive theories predict that even experts use theory-driven mental shortcuts to cope with the complexities and ambiguities of world politics, which allow them to: (a) make predictions on probable futures through the use of analogical reasoning; (b) make counterfactual inferences about plausible pasts; and (c) defend the products of analogical and counterfactual problem representation.<sup>3</sup> In order to improve policymakers’ ability to develop effective and efficient strategies attention must be paid to the cognitive process, information processing, and cognitive bias. Today, as historians and political psychologists review failed strategies, failed implementation of strategy, and operational failures such as the Bay of Pigs, the Iran-Contra affair, and Pearl Harbor, it has become clear that the idiosyncrasies of individual and group psychology can cause irrational decision-making, resulting in less than ideal outcomes. Cognition is central to the study of international affairs and decision-making, and underlies concepts such as power and interest.<sup>4</sup> Yet, despite the admonitions of political psychologists and some visionaries, decision-makers fail to appreciate the extent to which heuristics can give rise to systematic errors. As a result, many of their judgments continue to be marred by unintentional bias.<sup>5</sup>

## HEURISTICS: SHORTCUTS TO DISASTER?

Decision-makers are responsible for making rational and informed decisions on many significant situations that affect the nation’s interest. Rationality in decision-making results in foreign policy decisions based on facts, a ratiocinate analysis of information, and available choices while avoiding biases. Decision-makers have always experienced challenges meeting expectations due to the complexity and variability of the problems faced. Herbert Simon explained the possible source of the problem in his theory of “bounded” or limited rationality. He argued that the mind cannot cope directly



with the complexity of the world due to the limits in human mental capacity. To cope with this problem, humans develop simplified mental models of reality and then work with these models. People behave rationally within the confines of our mental model, but this model is not always well adapted to the requirements of the real world.<sup>6</sup>

Individuals assimilate and evaluate information through the medium of “mental models” or “mind-sets.” These models are experience-based constructs of assumptions and expectations about the world and more specific domains.<sup>7</sup> These mental models or shortcuts to interpreting information are referred to as “heuristics” by theorists. The variability in the tractability and ambiguity of strategic problems creates an environment which encourages the use of heuristics. However, the effectiveness of heuristics can be dependent on the accuracy of information and the quality of perception that created the model. This can be very tricky as it relates to strategy, as in many cases all the variables are not known; i.e., new information can be assimilated erroneously into existing models. Therefore, we are trying to fill gaps in information with information that also has gaps or errors. Even more problematic is the fact that decision-makers can become fixated on these mental models and preclude considerations of alternatives, reject contradictory information, or try to shape new information to suit the old model.<sup>8</sup> Stephen Marrin used the Greek word *scotoma* to describe this self-imposed blindness to considering new information and/or facts that contradict a previous hypothesis. This *scotoma* can cause decision-makers to reject, or forget, important or missing information that is not in accord with their assumptions and expectations. This is known as the *misinformation effect*, which is a result of a person incorporating “misinformation” into his/her memory of an event after receiving misleading information about it.<sup>9</sup> Consider the following example from World War II:

When the U.S. Secretary of the Navy was told of the Japanese attack on Pearl Harbor, he said, “My God, this can’t be true. This [message] must mean the Philippines.”

It is not without significance that the reaction is not that the report is incorrect, but that it *must* be incorrect.<sup>10</sup> This demonstrates the active-passive nature of perception that constructs rather than records reality. Perception is a deliberate process involving attention to a very small part of the whole and exclusion of almost all that is not within the scope of attention.<sup>11</sup> The resulting cognitive models help to centralize and unify objects, the state of affairs, sequence of events, and social and psychological actions.<sup>12</sup> However, as would be expected, these models

are often beset with pitfalls due to the limits associated with perception. The true problem arises for decision-makers as a result of the resistance of these quick-forming models to change as seen in the World War II example earlier. The resistance of the cognitive model to change gives rise to the majority of the problems associated with heuristics, which lead to *scotoma*.

## GROUPTHINK: COLLECTIVE DELUSIONS AND PERCEIVED ANONYMITY

Historical and laboratory evidence suggests that the decision-making process in development of foreign policies is undermined by a plague of chronic impediments, which negatively affect the quality of decisions.<sup>13</sup> These impediments include a lack of sufficient diversity of expressed opinions, excessive conformity in advisory groups, and the tendency of subordinates to tell the boss what they think he/she wants to hear. Cognitive biases in this case manifest themselves in organizational impediments, which distort a rational decision-making process. In situations in which there is a stressful policy environment, along with an “overly cohesive group,” these impediments can manifest themselves as a phenomenon referred to as “groupthink.”<sup>14</sup> Irving Janis defined groupthink as a process where group norms and patterns essentially take over and result in deeply flawed decision-making. Group uniformity is given priority over quality of information; competing hypotheses are ignored; dissent is discouraged, suppressed, or eliminated; shortcuts are taken in the process; and key assumptions are not thoroughly analyzed or critiqued.<sup>15</sup> The result of this flawed decision-making process is “premature consensus” on a skewed judgment based on insufficiently analyzed information.

---

***The most famous case of groupthink, the Bay of Pigs, demonstrates that even a team of exceptionally bright and talented individuals can succumb to a severely flawed decision-making process.***

---

The most famous case of groupthink, the Bay of Pigs, demonstrates that even a team of exceptionally bright and talented individuals can succumb to a severely flawed decision-making process. First, the Kennedy administration failed to question deeply flawed basic assumptions, due to a feeling of invulnerability and a “bounded” rationality that encouraged the administration to seek satisficing information. Second, it kept important information out of the process when it challenged the group consensus, effectively acting as self-appointed mindguards to “protect” the administration from dissenting opinions and information that

disputed the group's decisions.<sup>16</sup> President Kennedy, his brother Attorney General Robert Kennedy, and Secretary of State Dean Rusk all acted as mindguards during the decision-making process. President Kennedy, for example, withheld memoranda condemning the plan from both U.S. historian Arthur Schlesinger, Jr., and U.S. Senator William J. Fulbright.<sup>17</sup> Third, retrospective accounts reveal that there was self-censorship among individuals in the group. Many of the group members objected to the plan; however, this never came out in meetings.<sup>18</sup> Everyone wrongly assumed that the other members liked the plan, creating a false consensus. Lastly, conformity pressure was applied to individual dissenters, which quickly quieted anyone who dared to disagree with the President and others in the administration. Undersecretary of State Chester Bowles, who was notably against the course of action, was silenced in meetings held by Kennedy. Rusk intercepted his complaint to the committee about his misgivings regarding the plan and the action of his supervisor. Rusk even lied to Bowles, indicating that the plans had been changed.<sup>19</sup>

In the Bay of Pigs situation, failure to protect against group conformity during the decision-making process interrupted the critical thinking process and created an illusion of invulnerability, chronic stereotyping of the problem, and an "out group," plus strong pressures for uniformity against dissent.<sup>20</sup> This led to what Lucien Vandenbroucke, a Foreign Service Officer at the State Department, called the "Anatomy of a Failure." Group decisions are most likely to succeed in an environment where there are fluid lines of communication, structured analysis is conducted, and members feel free to speak candidly on the relative merits of the various policy options.

## WHAT DOES THIS MEAN AND WHAT CAN BE DONE?

Overall, there are many lessons that can be learned from understanding how humans think. Knowledge of the processes that provide structure to how we think, combined with a conscious effort to engage in meta-cognition, can improve the quality of decision-making. Psychoanalysts are required to undergo psychoanalysis themselves before obtaining their license in order to practice understanding how their own personality traits can potentially interact with and affect the perception of others. This ideology of understanding one's self to understand others should be considered by decision-makers.

In order to overcome the limitations inherent in human mental processes, decision-makers must adopt simple tools and approaches for overcoming these limitations

and think more systematically. Critical thinking is a cognitive process that may be able to provide the necessary improvement to the decision-making process, leading to more meaningful judgments. Critical thinking includes the component skills of analyzing, reasoning, judging, evaluating, making inferences, and making decisions or solving problems.<sup>21</sup> Critical thinking in itself will not magically lead to perfectly rational decision-making and by no means will it ensure the final decision will be "right." It will, however, ensure that decision-makers objectively use their experienced-based mental models while maintaining all pertinent and potential alternatives. Therefore, policymakers will avoid letting biases dictate what the information means, and will give due recognition and value to alternative competing hypotheses in order to mitigate rash judgments.<sup>22</sup>

---

*Critical thinking serves to improve the quality of reasoning through greater conscious attention to the process of thinking. It is the process of "thinking about thinking," or meta-cognition.*

---

Critical thinking serves to improve the quality of reasoning through greater conscious attention to the process of thinking. It is the process of "thinking about thinking," or meta-cognition. Critical thinking introduces strategies to develop skills that can be learned, mastered, and used. Critical thinking helps to use the inherent mechanism of information processing effectively by providing a framework to mitigate bias and ensure rational use of information. Critical thinking techniques provide a systematic approach that considers a range of alternative explanations and outcomes, and potentially prevents decision-makers from dismissing relevant hypotheses due to cognitive and perceptual bias.

Training is needed to increase self-awareness during the decision-making process and to provide the necessary guidance and practice in overcoming the potential problems with the process. This is especially important since the circumstances in which decision-makers have to make decisions are the most difficult for which to have an accurate perception: dealing with highly ambiguous situations on the basis of information that is processed incrementally under pressure for early judgment and often associated with high levels risk to the country and their careers. Decision-makers and their teams should be duly informed on the symptoms of the different types of biases and the structured critical thinking techniques that may be used to mitigate their effects. Techniques such as

Devil's Advocacy and Multiple Advocacy, which harness the power of conflict to provoke thought and mitigate the onset of groupthink, are very useful. These techniques allow decision-makers to navigate the fine line between the twin dangers of excessive conformity and destructive conflict among the policy advocates.

Cognitive psychology texts state that people have no conscious appreciation of most of what happens in the mind. Richards Heuer wrote, "Many functions associated with perception, memory and information are conducted prior to and independently of any conscious direction."<sup>23</sup> Weaknesses and biases exist in the human thinking process, and can create cognitive impediments to the individual or group; however, these cognitive errors can be alleviated by the conscious application of critical thinking tools and techniques. These tools and techniques should be kept in the mind of decision-makers when making their own final decisions or when creating and/or working with advisory groups to prevent the creation of implausible strategies and poorly considered foreign policy.

## NOTES

<sup>1</sup> Hammes, T.X., "Assumptions – Fatal Oversight," *Infinity Journal*, No. 1, Winter 2010: 4-6.

<sup>2</sup> Heuer, Richards J., *Psychology of Intelligence Analysis*, Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2001.

<sup>3</sup> Tetlock, Philip E., and Lawrence Freedman, *Theory-Driven Reasoning About Plausible Past and Probable Futures in World Politics: Are We Prisoners of Our Preconceptions?* Midwest Political Science Association, 1999.

<sup>4</sup> Young, Michael D., and Mark Schafer, "Is There Method in Our Madness? Ways of Assessing Cognition in International Relations," *Mershon International Studies Review* 42, 1998, no. 1: 63-96.

<sup>5</sup> Jones, Lloyd, *Patterns of Error: Perceptual and Cognitive Bias in Intelligence Analysis and Decision-Making*, Monterey, CA: Naval Postgraduate School, 2005.

<sup>6</sup> Heuer, Richards J., *Psychology of Intelligence Analysis*, Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2001.

<sup>7</sup> Heuer, Richards J., and Randolph H. Pherson *Structured Analytic Techniques for Intelligence Analysis*, Washington, DC: CQ Press, 2011.

<sup>8</sup> Cottam, Martha L., Beth Dietz-Uhler, Elena Mastors, and Thomas Preston, "Cognition, Social Identity, Emotions, and Attitudes in Political Psychology," in *Introduction to Political Psychology*, New York: Psychology Press, 2010.

<sup>9</sup> Ibid.

<sup>10</sup> Jervis, Robert, *Perception and Misperception in International Politics*, Princeton, NJ: Princeton University Press, 1976.

<sup>11</sup> Jones, Lloyd, *Patterns of Error: Perceptual and Cognitive Bias in Intelligence Analysis and Decision-Making*, Monterey, CA: Naval Postgraduate School, 2005.

<sup>12</sup> Johnson-Laird, P.N., *Mental Models: Towards a Cognitive Science of Language and Inference, and Consciousness*. Cambridge, MA: Harvard University Press, 1983.

<sup>13</sup> George, Alexander L., and Eric K. Stern, "Harnessing Conflict in Foreign Policy Making: From Devil's to Multiple Advocacy," *Presidential Studies Quarterly* 32, no. 3, 2002: 484-505.

<sup>14</sup> Hook, Steven W., "Understanding Foreign Policy Decision-Making," by Alex Mintz and Karl DeRouen; "Groupthink Versus High-Quality Decision Making in International Relations," by Mark Schafer and Scott Crichlow, *Political Psychology* 32, no. 5, 2011: 924-929.

<sup>15</sup> Schafer, Mark, and Scott Crichlow. *Groupthink versus High-Quality Decision Making in International Relations*. New York: Columbia University Press, 2010.

<sup>16</sup> Ibid.

<sup>17</sup> Forsyth, Donelson R., *Group Dynamics*, Pacific Grove, CA: Brooks/Cole Publishing Co., 1990.

<sup>18</sup> Ibid.

<sup>19</sup> Kramer, Roderick, "Revisiting the Bay of Pigs and Vietnam Decisions 25 Years Later: How Well Has the Groupthink Hypothesis Stood the Test of Time?" *Organizational Behavior and Human Decision Processes* 73, no. 2\3, 1998: 236.

<sup>20</sup> Hook, Steven W., "Understanding Foreign Policy Decision-Making," by Alex Mintz and Karl DeRouen; "Groupthink Versus High-Quality Decision Making in International Relations," by Mark Schafer and Scott Crichlow, *Political Psychology* 32, no. 5, 2011: 924-929.

<sup>21</sup> Hess, James Henry, *Improving Intelligence in a Counterinsurgency or Counterterrorism Environment through the Application of a Critical Thinking-Based Framework*, Baton Rouge: Louisiana State University, 2011. <<http://etd.lsu.edu/docs/available/etd-11022011-091541/>>.

<sup>22</sup> Ibid.

<sup>23</sup> Heuer, Richards J., *Psychology of Intelligence Analysis*, Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2001.

*Troy E. Smith, a citizen of the Caribbean nation of Trinidad and Tobago, entered the field of intelligence in 2008 upon joining the Security Intelligence Agency of that country. His initial position was as an intelligence officer. Subsequently, he embarked upon several training endeavors, both regionally and internationally. As an analyst he has written a number of papers on the intelligence activities of the Chinese, on cybercrimes, and on the insider threat. After beginning work on an MA in Intelligence Studies degree at American Military University in the U.S., he chose to focus on the area of intelligence collection. Troy represents his agency on several committees and has served in various command centers over the last seven years. He is a frequent and valued contributor to AIJ.*



---

# Demographics and Conflict

by Dr. Michael M. Andregg

---

## INTRODUCTION TO AN ANCIENT PARADIGM: POPULATION GROWTH, ENVIRONMENTAL DEGRADATION, RISING DEATH RATES AND CONFLICTS, EXODUS, WAR, OR GENOCIDE

People have been killing each other since before the beginning of written history, as recorded by the broken bones of people massacred long before writing was invented.<sup>1</sup> One of the quiet reasons for the large-scale killings known as genocides and wars is demographics—the statistics of birth rates, death rates, growth rates, and migrations into or out of territories.<sup>2</sup> This dimension is under-covered by those who focus on the statements or acts of key leaders. Politicians and commanders of war typically have described their reasons in political, religious or military terms, not in demographics. However, they were also often driven by forces they barely understood and could not control. The Mayan Empire probably fell that way. Easter Island certainly did. Moreover, the deserts of North Africa are filled with ruins from cities and empires that thrived...before the forests and farmable land turned into desert. The Kenyans have a saying: “First came forests, then man, then the deserts.”

Therefore, this article will show how simple births, deaths, and migrations lead to an iron law of biology. This law observes that all living populations eventually achieve equilibrium with their environment, which means birth rates equal death rates and the population neither grows nor declines, or they die. Populations that try to grow forever suffer catastrophic death rates or become extinct. The modern case of Syria disintegrating after 2010 will be considered in some detail, because it also shows how other global factors like climate change can trigger chaos.<sup>3</sup> Syria’s population growth rate in 2011 was 2.4% per year, but when half of its population was displaced by civil wars and about 6 million fled, its growth rate became sharply negative. At least 450,000 people died by violence alone.

This will be followed by a short section on “Human Nature, Nurture, Free Will, and War” because that topic

has generated much commentary over the centuries, with large implications if one accepts the simplistic conclusions that people are either born “innately” warlike, or instead “innately” social and cooperative. The truth is that people can be either one or the other depending on circumstances, and on that much neglected factor: “free will” or personal decisions. Finally, we close with how a few more complicated demographics such as “pyramidal” vs. “columnar” age distributions and distorted gender ratios may influence the probability of organized armed conflict on earth today and in the future.

## AN IRON LAW OF BIOLOGY

It has been known for millennia that everything born (on earth anyway) eventually dies. Therefore, in the long run, birth rates must equal death rates for living populations. Nevertheless, the peculiar history of human populations can make the implications of this simple fact hard to see. Human populations remained about the same for thousands of years, at near equilibrium with their environments, then started growing almost continuously after agriculture improved and science made huge advances in health care and much more. This leads some people to conclude that growth is inevitable, for humans, and that we do not have to worry about limits.

That is a big mistake, because it turns out that one of the consequences of the iron law is that, in the long run, in equilibrium populations, birth rates determine life expectancy. This means that you can have low birth rates and low death rates, or high birth rates and high death rates (which lead to low life expectancy), but you cannot have high birth rates and low death rates for very long without destroying your environment, which greatly increases death rates.

More specifically, in a stable equilibrium population that neither grows nor shrinks and is uncomplicated by migration flows or unstable age distributions, the life expectancy (LE) is equal to 1,000/death rate. Hence, a death rate of 14 per thousand per year, for example, would yield a life expectancy of a little over 71 years (71.3 years = 1,000/14). Since this population is in equilibrium, death



rates equal birth rates, which as a practical matter means that birth rates determine life expectancies, unless you intend to invade neighbors and take their land or other resources. If so, a militant population can grow larger for a while, but it can never escape the iron law of biology. Consequently, empires rise, but always fall too, in a short time period on the scale of civilizations.

This concept is especially important in our modern world because people everywhere naturally want to control death rates through modern medicine and effective health care. Deliberate birth control programs (much less government-mandated birth control like China has, or had until recently) are much more controversial than reducing death rates. Ignoring this factor leads to famine, war, and genocides, however. For another example, consider the U.S. state of Minnesota. Census records show that the territory of Minnesota was 99% Native American in 1800, with 1% whites of European descent. A phenomenal reversal occurred in just one century. In 1900 Minnesota's population was 99% white, with the remaining 1% divided about equally between Native Americans and blacks.<sup>4</sup> The biggest single factor was immigration of millions of people fleeing problems in Europe for opportunities in America, which included occupying most of the land of Minnesota and displacing much of the native population by war (in 1862) and thousands of smaller violent encounters.

## ENVIRONMENTAL CONFLICT AND MASS MIGRATIONS: SYRIA AS AN EXAMPLE

**D**amascus, the capital of modern Syria, is one of the oldest cities in the world. However, Syria is a nation that may not survive another ten years much less 8-10,000 years. Recent governments were always authoritarian and sometimes brutal. For example, the current leader's father, Hafez al-Assad, killed about 20,000 people in one city called Hama while suppressing a rebellion in 1982. Things were going pretty well for the son and current leader, Bashar al-Assad, and for the country overall which had solid education and professional skills, until the situation started falling apart in the 21<sup>st</sup> century. Let us look briefly at how demographics matter there.

In 2011 the United Nations<sup>5</sup> and the CIA<sup>6</sup> reported that Syria had a population growth rate of 2.4%, which means it would double in about 30 years. It is very hard to feed a population that doubles every 30 years, even if the land is fertile and vast. The entire earth's population also grew, from one billion in 1804 to over seven billion in 2011. This growth used the best farmland, and increased use of fossil fuels led to global warming and climate change. The worst drought in the history of local weather

record-keeping came to Syria, making much of its farm land infertile. This led to a minimum of 1.5 million of Syria's then 23 million people migrating from farms into cities seeking opportunity. Yet, the young Assad could not employ all of the young men and women already coming of age in cities like Damascus. Being dictatorial, he was keeping the best opportunities for members of his minority, the Alawite group, and also minority Christians who supported him, because he was known for protecting minorities in a Middle East better known for exterminating them. Consequently, protesters were frustrated, while agriculture failed.

---

***Damascus, the capital of modern Syria, is one of the oldest cities in the world. However, Syria is a nation that may not survive another ten years much less 8-10,000 years.***

---

High growth rates also result in "pyramidal" age distributions where the young greatly outnumber the old. In Syria this meant half of the population was less than 22 years old in 2011. Pyramidal age distributions have especially bad consequences when millions of teenaged males cannot find good job opportunities or farmland to support a family. Demagogues abound who will try to focus this frustration on neighbors, blamed for all the problems. Peaceful protests began in Syria about 2011; however, because Assad could not create jobs or good farmland out of dry air, protests were repressed in the "normal," authoritarian ways. Yet, desperate migrants kept coming into the cities, where desperate teens were watching their dreams of good jobs and families evaporate. Therefore, the protests did not stop, and violence escalated until complex civil wars emerged, involving many factions and outside groups which killed at least 450,000 people and displaced about half of Syria's residents. Approximately six million left the country entirely—a million to Lebanon, over three million to Turkey, 635,000 to Jordan—and another million passed through these border countries to other destinations including Western Europe. This puts huge strains on destination countries even if major donors pay to feed people in refugee camps, which is not always the case. True settlement and assimilation take much more money, and time.

By 2015 a desperate migration began<sup>7</sup> where over one million refugees fled toward Europe, on foot and in tiny boats, not all from Syria but many from other desperate

war zones enduring similar underlying conditions, like Iraq and Afghanistan. This phenomenon has terrified some Europeans. This is how population growth turns into population pressure, which can turn into a catalyst for either great positive changes or global war depending on the details of conflict and the leadership on which many scholars focus.

## HUMAN NATURE, NURTURE, FREE WILL, AND WAR

The history of humankind includes at least 3,000 wars and many times more riots, insurrections, police-state repressions like the 20,000 killed in Hama, Syria, or the tens of millions killed in Stalin's Soviet Union and Mao's China. Millions of Native Americans have been displaced by surging white populations since 1492, few of which are included in technical definitions of war.

This bloody history has generated much commentary for thousands of years on whether or not war is inevitable. Such scholars often focus on human nature, and whether humans are "genetically" or "innately" destined for war. The most quoted passage in a previous work by this author, "On the Causes of War,"<sup>8</sup> concluded: **War is not inevitable. Human conflicts are inevitable, but war is not. War is a social institution. Institutions have been created by people. Therefore, they can be changed.**

This is not the place for a technical discussion of behavior genetics, but the bottom line deserves some emphasis. Most scholars talk about "nature" and "nurture" as though these were the sum of all causes, but there are assumptions in that paradigm that fall apart when examining complex traits of human behavior. War is an excellent example. What is missing from the simple nature/nurture paradigm is the clearly demonstrated ability of people to decide for themselves whether they will participate in war, or work for peace, or whatever. This applies to top leaders who actually make the decisions and give the orders necessary to start wars, as it does to citizens.

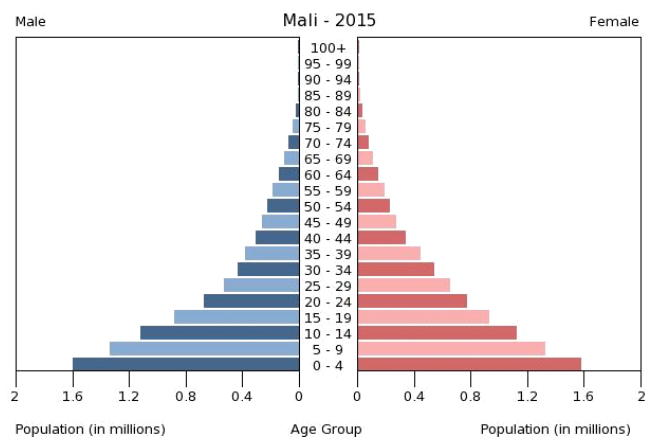
The big problem with "inevitability" is that it traps people who feel powerless, and excuses others who like, want, and sometimes start wars for personal profit or glory. Therefore, I ask the reader to go back two paragraphs and reread the bottom line regarding conclusions on inevitability.

## AGE DISTRIBUTIONS, AND OTHER ODDITIES LIKE DISTORTED GENDER RATIOS

We have already mentioned age distributions; thus, it is time to look at two. The first is a "pyramidal" age distribution from a fast-growing population in 2015, Mali. The second is a "columnar" age distribution from a near zero growth population in Northern Europe—Sweden. The former has high growth rates, low average age, low average life expectancy, and severe "momentum of growth" since so many of its young are entering reproductive ages. Columnar age distributions yield low growth rates, higher average ages, and much higher life expectancies.

*Mali is a very poor country in an area of endemic armed conflict and spreading deserts. Sweden is a very rich country in an area of no wars (since 1945) and no deserts.*

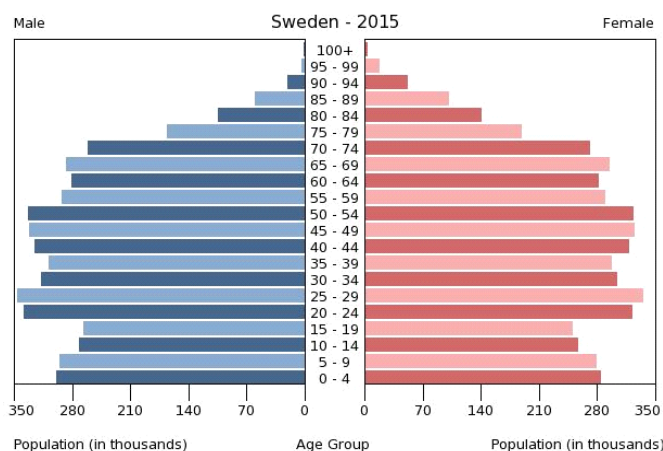
Mali is a very poor country in an area of endemic armed conflict and spreading deserts. Sweden is a very rich country in an area of no wars (since 1945) and no deserts. Mali has very high birth rates, correspondingly high death rates, and low life expectancy, with Sweden the reverse. More specifically, in 2015 the CIA reported<sup>9</sup> (based largely on UN demographic data) that Mali's birth rate was 45/ thousand, from a total of 17 million people, a growth rate of 2.98% per year (doubling every 23.5 years), a median age of 16.1 years, a life expectancy of 55.34 years, and Mali was exporting people to its neighbors at a rate of 2.56 per thousand each year by emigration.



**Caption for both age distributions, from the CIA's *World Factbook*: "A population pyramid (or age distribution)**

illustrates the age and sex structure of a country's population and may provide insights about political and social stability, as well as economic development. The population is distributed along the horizontal axis, with males shown on the left and females on the right. The male and female populations are broken down into 5-year age groups represented as horizontal bars along the vertical axis, with the youngest age groups at the bottom and the older at the top. The shape of the population pyramid gradually evolves over time based on fertility, mortality, and international migration trends."

For contrast, Sweden's population was 9.8 million, with a birth rate of 12 per thousand, a growth rate of .8% per year, a median age of 41.2 years, and a life expectancy of 82 years. Furthermore, Sweden is not exporting people, but rather attracting them. Its net immigration rate in 2015 was 5.42 migrants per year per thousand of population. Thus, Sweden has lower birth rates, a smaller population, a much longer life expectancy, and is a place people immigrate to, rather than emigrate from.



We mention one more complication here because it *may* influence the probability of wars. This is distorted gender ratios such as the fact that China today has about 120 male babies for every 100 female babies reported. This is not natural, but is a result of selective abortions and even killings of baby girls. Partly this is an unintended result of a once very strict "One Child" policy China employed to restrain its population growth, end periodic famines, and allow prosperity. Yet, *China is not alone; India also has a severely distorted gender ratio among the young.* It is possible, but not proven, that having many teenaged males who will never form a traditional family due to such differences in numbers may lead to more urban crime and even more aggressive foreign policies. These are other problems demographers worry about when considering the fate of nations.

## CONCLUSIONS

Demographics are destiny. This overstatement captures a powerful partial truth. Of course, there are many other factors that determine the fates of nations and people, including the personalities of leaders, historical and geopolitical context, military factors, economics, water, philosophy, and all the rest. Life is complicated, and the phenomena of wars and other organized armed conflicts are hyper-complicated because they involve institutions as well as people, and factors like demographic variables and climate (especially changes) as this chapter has shown.

Consequently, demographics do not determine *all* of destiny, just some of it. However, these powerful forces are typically invisible, or drowned out by endless discourse on political, military, and religious perspectives. We have tried to show here how birth rates also have powerful effects on political, military, and even religious realities on earth today. We will close with one other complication from behavior genetics and anthropology.

Humankind evolved in a context of many small groups that depended on each other for survival, and were fed mainly through hunting and gathering rather than settled agriculture. There were lots of other predators about, like real lions, tigers, and bears, and people moved a lot because hunters and gatherers typically use up most of the food in any one area over time. Therefore, our ancestors encountered other groups of people as well as other predators, on the move seeking new resources. Sometimes they fought and sometimes losers were massacred. This resulted in an almost universal double standard of "in" groups vs. "out" groups, which has been studied by sociologists and psychologists as well as those from the other fields mentioned. With regard to war and conflicts similar to war, that in group/out group concept reflects this specific consequence.

We have endured thousands of years of smaller, weaker, or merely gentler people being wiped out by more aggressive neighbors. This reinforces the ancient paradigm of loyalty to family, clan, or tribe and a certain reflexive aggressiveness if large numbers of strangers begin to appear. Threats are implied (by some) before they are real, and strangers are often considered barbaric and dangerous before they are even known.

For millennia we, as a species, could endure the endless wars, genocides, and lesser conflicts that resulted. However, weapons of mass destruction (WMDs) have changed all that. Actually wiping out entire populations has become much less practical and considerably more dangerous. No matter how barbaric "they" are, they are

people too, with eyes to see and brains that can make weapons for themselves. Therefore, human civilization—the global civilization emerging from ancient ones now clashing vigorously—is rethinking how to achieve security in an age of WMDs and grave changes in the natural environment with large effects on economic growth and military power. It is a time of great peril and, as the Chinese say, great opportunity.

What we do about all that is up to us.

## NOTES

<sup>1</sup> *The New York Times* editorial board, “Is Warfare in Our Bones?” January 24, 2016, p. SR12. An associated article is by James Gorman, “Prehistoric Massacre Hints at War among Hunter-Gatherers,” in *The New York Times*, January 20, 2016, p. A-7, or [http://www.nytimes.com/2016/01/21/science/prehistoric-massacre-ancient-humans-lake-turkana-kenya.html?\\_r=0](http://www.nytimes.com/2016/01/21/science/prehistoric-massacre-ancient-humans-lake-turkana-kenya.html?_r=0).

<sup>2</sup> Andregg, Michael M., *Seven Billion and Counting: The Crisis in Global Population Growth*, Minneapolis, MN: Twenty-First Century Books (an imprint of Lerner Books), 2014.

<sup>3</sup> Liverani, Andrea, “A Syrian Refugee at COP21,” in the World Bank blog, accessible at: <http://blogs.worldbank.org/peoplemove/syrian-refugee-cop21>.

<sup>4</sup> Primary census data for Minnesota is obtainable from the Minnesota Population Center. This was originally a department of the state government now housed at the University of Minnesota, <https://www.ipums.org/>.

<sup>5</sup> United Nations, *Demographic Yearbook*, 2013 is the latest published, accessible at <http://unstats.un.org/unsd/demographic/products/dyb/dyb2013.htm>.

<sup>6</sup> The CIA’s *World Factbook* has basic demographic data for all countries available, by year, including age distributions and

enormous amounts of other practical information. This useful resource is published annually in book and online forms by the U.S. Central Intelligence Agency.

<sup>7</sup> UN High Commissioner for Refugees, “UNHCR Syria Regional Refugee Response/Total Persons of Concern,” accessed at: <http://data.unhcr.org/syrianrefugees/regional.php> on January 22, 2016.

<sup>8</sup> Andregg, Michael M., *On the Causes of War*, St. Paul, MN: Ground Zero Minnesota, 1997, 2001. Chapters on “Population Pressure” (pp. 62-73) and “Human Nature, Nurture, Free Will and War” (pp. 26-29) are especially relevant here.

<sup>9</sup> All material here, including birth rates, growth rates, migration rates, life expectancies, two age distributions of Mali and Sweden, and corresponding text on what age distributions (or population pyramids) mean, are from the CIA’s *World Factbook* of 2015. Much (not all) of the primary demographic data comes from the UN Demographic Unit, but the UN does not have enough staff to compile an annual report like the CIA does.

*Dr. Michael M. Andregg is an adjunct instructor in the Aquinas Scholars Honors Program at the University of St. Thomas in St. Paul, MN. He has also been an adjunct in the Graduate School of the University of Minnesota since 1981, and currently teaches in the Master of Liberal Studies Program there. He is a specialist in the causes of war.*



# JOIN US



NMIA is a non-profit voluntary professional association based on the fundamental proposition that sound military intelligence is essential to national defense, security, liberty, and peace. Our goal is to foster the professional development of all members of military intelligence, support all those who provide intelligence in defense of our nation, and ensure clear public understanding of the critical role and value of military intelligence. For more information please visit the NMIA website at:

[www.nmia.org](http://www.nmia.org)



---

# Lanes in the Road:

## Streamlining Intelligence Community Congestion

by (LTC, USA, Ret) Thomas M. Cooke

---

**T**he United States Intelligence Community (IC)<sup>1</sup> is attempting to address 21<sup>st</sup> century asymmetrical intelligence challenges using a 20<sup>th</sup> century construct that is too rigid and parochial to allow for real change. As intelligence requirements continue to evolve in an environment of budget austerity, Congress will demand a stronger accounting of expenditures with demonstrable results. The U.S. can no longer afford to accept the redundancies and mission creep that continue to characterize the IC in the post-9/11 world.

---

*The U.S. can no longer afford to accept the redundancies and mission creep that continue to characterize the IC in the post-9/11 world.*

---

With the cessation of U.S. ground combat operations in Iraq, the death of Osama Bin Laden (OBL), the impending withdrawal of combat forces from Afghanistan, and the current focus on the so-called Islamic State, the IC is again at the threshold of potential change. While the IC did indeed enact minor changes following the end of the Cold War, in the wake of the attacks on 9/11, and in preparation for the invasion of Iraq, a different change agent is now at work: pressure for major funding cuts to all federal programs. Political bellwethers now predict decreasing budgets as the norm for the next several years. Agencies accustomed to Overseas Contingency Operational (OCO) funds must now maintain initiatives within their normal Program Objective Management (POM) processes,<sup>2</sup> and Congressionally-mandated sequestration has forced major decreases in both National Intelligence Program (NIP) and Military Intelligence Program (MIP) funding.

With impending fiscal constraints, it would seem logical for the IC to develop a centralized approach to help mitigate any overall impact; yet, no one is in charge. Each IC member remains free to determine what it will analyze and report. While the creation of the position of Director of National Intelligence (DNI) offered the potential for effecting meaningful change by providing far-reaching oversight, in practice ODNI remains primarily an advisory board with little

ability to affect how IC organizations spend the money they receive from various sources. IC members receive their funding either directly from Congress or as line items within the Department of Defense (DoD) budget, and to maintain that funding stream they must continually justify their budget allocation by proving their relevance, particularly to the President or other senior members of the National Command Authority (NCA). As a result, IC organizations routinely provide individual assessments on the latest strategic-level activities reported within the past 24-hour news cycle, and much of it is uncoordinated. Reports routinely surface that may not have been previously coordinated with the organization(s) normally responsible for that type of reporting.

The situation is analogous to driving on a multi-lane highway. On a highway, if you wish to change lanes, you look ahead, behind, and adjacent to you, signal your intention to change lanes, move into the lane, and then, when appropriate, return to your previous lane. If everyone drives in the same lane, traffic slows and the potential for accidents increases. It is the same within the IC, except without the rules of the road. There is no requirement to signal a “lane change”; organizations “change lanes” based on the latest news event, and soon everyone is driving in the same lane<sup>3</sup> with resultant duplication and often competing analysis<sup>4</sup> that is neither healthy nor cost-effective.

The current processes are inefficient, and the IC must be prepared to conduct a self-assessment of the way in which it responds to the Key Intelligence Questions (KIQs) being asked of it. A potential first start should include at minimum a review of each IC agency and how it conducts intelligence-gathering and reporting. This should be followed by inducing rigor into the process by which IC organizations report on critical issues. Such a review—without the burden of internecine fighting or institutional bias—could result in significant efficiencies and cost savings without negative impact on overall intelligence support to the NCA. Finally, the IC should be prepared to discuss the demarcation between intelligence collection and analysis and the actual conduct of military-style combat operations by some of its members.

---

## FROM THE BEGINNING

If past is prologue, it is useful to review the evolution of the IC from its post-World War II inception to determine whether change is possible within the current structure or if a major reconsideration of the IC foundation is in order. Using the 1947 National Security Act as the IC genesis, it is clear the Soviet Union was the primary threat for which the initial structure was established. The war had just ended and, while a military downsizing was clear, the looming threat from Moscow made the military services loath to disband the robust intelligence capabilities they had developed. MG (USA) William Donovan, who had created and led the Office of Strategic Services (OSS), recognized the value of maintaining a clandestine operations capability in the post-war era and recommended the U.S. replicate a capability similar to the United Kingdom's Secret Intelligence Service (MI-6). With the war over, however, the OSS was disbanded and its mission split between the War Department's Strategic Services Unit (SSU) and the State Department's Interim Research and Intelligence Service (IRIS).<sup>5</sup> In this construct, a structure existed whereby the SSU could provide assessments on the Soviet Union's military "capability" and the IRIS could provide analysis on Moscow's strategic "intent."

In late 1945 Navy Secretary James Forrestal commissioned a study that recommended unifying the military services and developing a National Security Council (NSC) and a Central Intelligence Agency (CIA).<sup>6</sup> President Truman reviewed the recommendations and in 1946 authorized the creation of the National Intelligence Authority, a Central Intelligence Group (CIG), and a Director of Central Intelligence (DCI).<sup>7</sup>

The CIG was responsible for coordinating, planning, evaluating, and disseminating intelligence. It was not an independent organization but comprised of elements from other departments. It played a minor role in foreign policy assessments compared to the IRIS. When Congressionally-mandated budget cuts in 1946 reduced the size of the State Department, many IRIS analysts were transferred to other organizations, to include the CIG. Without a robust IRIS, there was now no single government organization to provide strategic assessments on Soviet intentions.

In July 1946 President Truman granted the DCI additional authority to "accomplish the correlation and evaluation of intelligence relating to national security."<sup>8</sup> Using the CIG as a template, the first DCI, Admiral Sidney Souers, argued against the now smaller State Department IRIS managing foreign intelligence and successfully lobbied for creating a Central Intelligence Agency (CIA).<sup>9</sup> The new CIA became codified within the 1947 National Security Act "to advise the NSC in matters concerning such intelligence activities of the government departments and agencies as (to) relate to

national security."<sup>10</sup> The CIA was specifically precluded from any police or law enforcement activities<sup>11</sup>; however, the Federal Bureau of Investigation (FBI) would provide information to the DCI "upon request."<sup>12</sup> The National Security Act also established a Department of Defense (DoD) comprised of the military services (Army, Navy, and newly formed Air Force) led by the new Cabinet-level Secretary of Defense (SECDEF).<sup>13</sup>

---

***DIA was officially established on 1 August 1961 with the charter to provide the NCA all DoD-level estimative and current intelligence.***

---

The post-war period also included an effort to coordinate the independent Navy and Army military communications intelligence (COMINT) capabilities. Throughout the late 1940s the newly formed NSC attempted to coordinate the services' COMINT capabilities with such organizations as the U.S. Communications Intelligence Board (USCIB) and the Armed Forces Communication Intelligence Agency (AFCIA)—later renamed the Armed Forces Security Agency (AFSA). AFSA operated until 1951 when President Truman, reacting to intelligence challenges revealed during the Korean conflict, commissioned the "Brownell Committee" to determine how to better integrate service-level COMINT with other intelligence efforts.<sup>14</sup> The National Security Agency (NSA) was subsequently chartered in 1952 to ensure national-level COMINT was "organized and managed as to exploit to the maximum the available resources of all participating departments and agencies."<sup>15</sup>

Throughout the 1950s the military services continued to develop and report their own assessments of foreign military capabilities. These often proved contradictory, and before leaving office President Eisenhower commissioned a Joint Study Group under Lyman Kirkpatrick to develop a way in which to consolidate General Military Intelligence (GMI) reporting. The Joint Study Group recommended a single intelligence organization under the DoD, and in 1961 SECDEF Robert McNamara directed the Joint Chiefs of Staff (JCS) to develop a conceptual Defense Intelligence Agency (DIA).<sup>16</sup> DIA was officially established on 1 August 1961 with the charter to provide the NCA all DoD-level estimative and current intelligence.<sup>17</sup>

Various executive orders and Congressional actions directed other significant changes within the IC and military departments. For example, the 1949 CIA Act<sup>18</sup> further codified the CIA's ability to protect its internal administrative actions and funding activities from public scrutiny, and the 1986 Goldwater-Nichols Act improved joint

operations and streamlined the military command structure.<sup>19</sup> Most recently, the 2004 Intelligence Reform and Terrorism Prevention Act and related legislation created the Department of Homeland Security (DHS); authorized new intelligence centers, such as the National Counterterrorism Center (NCTC)<sup>20</sup>; and granted other agencies additional authorities and powers, such as the FBI developing a “national intelligence workforce.”<sup>21</sup> With new missions and additional agencies, the IC no longer resembled its originally envisioned structure.

## THE COLD WAR IS OVER

The 1990 demise of the Soviet Union caused the IC, or its individual components, to reassess their business models and address a major challenge: how to remain relevant in an era of anticipated shrinking budgets without a major adversary against which to focus. The U.S. agreed to reduce its conventional military presence in Europe<sup>22</sup> and efforts began to consider the future in the context of asymmetrical warfare.<sup>23</sup> Congress and the American people demanded a “peace dividend” and expected the IC, to include its components within the military services, to downsize.<sup>24</sup>

Although the 1991 Gulf War provided a short resurgence in discussing the need for a strong conventional military capability, a discourse on the “Revolution in Military Affairs,” or RMA,<sup>25</sup> emerged. Military and civilian leaders no longer focused on major land warfare, and smaller conflicts, from Somalia to Bosnia-Herzegovina, began to drive U.S. foreign policy. Congress recognized the need to review “business as usual” and started to look for ways to experience the budget savings promised by the RMA paradigm.

The challenge for the IC members was clear: with a potentially shrinking budget, how could current analytic capabilities and tradecraft be focused against a non-traditional adversary while maintaining the same level of national security and retaining the ability to surge in the event of a potential global conflict? IC leaders argued that because a “potential” adversary could still arise they needed to maintain the diligence necessary to guard against a strategic surprise, a debate now complicated by the absence of a major military antagonist. The Chinese were emergent but not yet peer competitors or sufficiently adversarial to justify maintaining the IC status quo. CIA, NSA, and DIA all agreed that each of the intelligence disciplines, or “INTs,” for which they were responsible needed to remain fully capable of providing strategic warning. Each IC agency initiated efforts to ensure major programs remained intact, and as a result continued to operate under its former constructs using the processes and databases with which it was most familiar. CIA maintained its clandestine Human

Intelligence (HUMINT) efforts; NSA remained focused on Signals Intelligence (SIGINT); and DIA continued its General Military Intelligence (GMI) mission, its overt HUMINT collection efforts through the Defense Attaché System, and its technical Measurement and Signatures Intelligence (MASINT) role.

---

*With the DCI also leading the CIA as an individual agency, the latter was perceived within the IC as first among equals, a concern posited as early as 1976 by the Pike Committee.*

---

Throughout the IC budget scrutiny, CIA continued to maintain a premier position due largely to its Director being dual-hatted as DCI.<sup>26</sup> With the DCI also leading the CIA as an individual agency, the latter was perceived within the IC as first among equals, a concern posited as early as 1976 by the Pike Committee.<sup>27</sup> The DCI’s statutory responsibility as the senior intelligence advisor to the President resulted in primary intelligence support to the NCA becoming almost indistinguishable from the CIA. The President’s Daily Briefing (PDB), for example, served as a daily all-source document produced for the President and members of the senior NCA staff. Although the PDB eventually included input from across the IC, for years CIA analysts primarily used CIA-collected data to compile, edit, and brief the PDB contents.<sup>28</sup> CIA also benefited by an overall IC shift from traditional GMI analysis to a more asymmetric focus. As non-state actors gained prominence on the world stage, clandestine HUMINT sources became critical and, despite an overall 16 percent cut in CIA’s budget, IC-level counterterrorism funding tripled and CIA counterterrorism funding quadrupled.<sup>29</sup>

DIA continued its full GMI mission but now struggled with self-identity. Many within the IC perceived DIA as a Cold War legacy, with the need for “bean-counting” military equipment less relevant in an asymmetric environment. Each of the combatant commands (CCMDs) was now considered the appropriate organization to monitor military activities within its respective area of responsibility (AOR) using Joint Intelligence Centers (JICs).<sup>30</sup> DIA’s requirement to maintain major portions of the Modernized Integrated Database (MIDB) was delegated to other organizations now designated as Responsible for Production (RESPROD) under the Defense Intelligence Production System.<sup>31</sup> There was less need for DIA analysts to monitor Russian T-72 tanks when the same mission was performed at the U.S. European Command in Stuttgart, Germany. Thus, DIA

began to focus on other national-level activities to include counterdrug and counterinsurgency operations—with a workforce trained to monitor military organizations and (primarily idle) Russian tanks, ships, and submarines.

Nor was NSA spared post-Cold War budget scrutiny. Without the Soviet Union, many began to question whether NSA needed to maintain a large cadre of analysts specifically targeted against what was now considered a benign adversary. The Director of NSA (DIRNSA), whose authorities included oversight of tactical SIGINT efforts performed by the military services,<sup>32</sup> eventually experienced a one-third decrease in overall manpower and budget.<sup>33</sup>

The sole “INT” without a champion was Imagery Intelligence (IMINT). The Gulf War and conflicts within the Former Yugoslavia revealed several flaws in the way imagery intelligence and geospatial information supported both warfighters and policymakers. IMINT was performed within many IC organizations, and there was no standard by which to incorporate it in concert with standard maps and map-like products. The IC recognized this dysfunction and petitioned Congress to enact legislation bringing these processes together. In response, in 1996 Congress created the National Imagery and Mapping Agency (NIMA)<sup>34</sup> to focus and manage imagery, imagery intelligence, and geospatial information into what would soon be termed geospatial intelligence (GEOINT). There was now one organization responsible for coordinating imagery and geospatial intelligence in support of DoD and national-level intelligence requirements.

NIMA realized cost savings across the IC, at least in overhead: NIMA fully incorporated the Defense Mapping Agency (DMA), the Central Imagery Office (CIO), the Defense Dissemination Program Office (DDPO), and the CIA National Photographic Interpretation Center (NPIC), in addition to including the imagery assets of DIA, the National Reconnaissance Office (NRO), and the Defense Airborne Reconnaissance Office (DARO). Under former DMA Director RADM Joseph Dantone, NIMA was chartered as both a combat support and national intelligence agency to respond directly to taskings from both the SECDEF and the DCI.

## POST-9/11 AND CONNECTING THE DOTS

The 11 September 2001 attacks jolted the U.S. with its loudest wake-up call since Pearl Harbor. This was indeed a case of strategic surprise, and many began to question how the world’s only superpower could have been caught so off-guard. Both Congressional intelligence committees initiated a Joint Commission to investigate whether the attacks were due to what the forum of public opinion considered a massive intelligence failure.

The resultant *9/11 Commission Report* faulted the IC for its failure in “connecting the dots.”<sup>35</sup> Intelligence reporting remained within “stove-pipes,”<sup>36</sup> with agencies failing to share information that could have helped identify the events and actions leading up to the aircraft hijackings. Agencies were directed to remove impediments to information sharing and develop “information procedures (to) provide incentives for sharing, to restore a better balance between security and shared knowledge.”<sup>37</sup>

---

### ***What the DNI did not receive under the Intelligence Reform and Terrorism Prevention Act was full development and implementation authority over the total IC budget.***

---

The *9/11 Commission Report* also called for a more centralized IC management approach. Specifically, the report recognized the challenge of the IC managed by a DCI with “too many jobs.”<sup>38</sup> DCI responsibilities since 1947 had expanded significantly. For example, in addition to managing the CIA, the 1978 EO 12036 increased DCI authorities over the IC for “budget, tasking, intelligence review and coordination and dissemination,”<sup>39</sup> and the 1981 EO 12333 designated the DCI the “primary intelligence advisor to the President and the NSC on national foreign intelligence.”<sup>40</sup> The *9/11 Commission Report* also recognized the “divided management of national intelligence capabilities”<sup>41</sup> and called for replacing the DCI with an independent “National Intelligence Director” with appropriate statutory authority to “manage the intelligence program and oversee the agencies that contribute to it.”<sup>42</sup>

In 2004 Congress passed the *Intelligence Reform and Terrorism Prevention Act*,<sup>43</sup> based largely on the findings and recommendations of the *9/11 Commission Report*. This legislation modified the National Security Act of 1947 by establishing a Director of National Intelligence (DNI) to serve as the head of the IC and principal intelligence advisor to the President and the NSC. The DNI was ceded all authorities previously assigned to the DCI and granted authority over the newly created National Counterterrorism Center (NCTC), as well as given the ability to create other centers as required. Of note, the DNI was specifically precluded from leading any other intelligence agency.<sup>44</sup>

What the DNI did *not* receive under the *Intelligence Reform and Terrorism Prevention Act* was full development and implementation authority over the total IC budget. While the DNI may provide guidance to NIP-funded IC members as they develop their individual budgets, the position has no statutory oversight of the MIP, for which the SECDEF



retains full oversight and responsibility. The SECDEF is required only to “consult” with the DNI, which precludes the DNI from fully implementing a national-level IC budget and program. The DNI also has no direct operational control over MIP funding; the SECDEF provides these funds to the military services, and they in turn have operational control over resource allocation. As demonstrated during the FY13 Congressional sequestration, the DNI does not have the authority to manage MIP-funded intelligence personnel, which led to furloughs for MIP-funded IC members but not those funded under the NIP.

### **POST-OBL AND SEQUESTRATION— FOCUSING ON THE BASICS: CAPABILITY AND INTENT**

**T**he question now before the IC is not whether to restructure, but how. The IC is capable of moderate change; it enacted change in the 1990s after the Cold War and again restructured after the 9/11 attack. Given a fluid world order and an austere fiscal future, it is now imperative to review whether the IC should conduct another readjustment or perhaps undergo a major transformation. A full review of the role of the IC in support of the national elements of power (e.g., DIME: Diplomatic, Information, Military, Economic) is worthwhile, and a return to the basics might help frame the discussion.

At the basic level, intelligence structures exist to provide answers to questions on potential adversaries’ leadership, political motivations, military capabilities, industry, businesses, and their practices, as well as provide context as it relates to geography, weather, socio-political issues, etc. Regardless of the intelligence topic, two major tenets are inherent in all questions: capability and intent. Can an enemy attack (capability) and will it (intent)? Can a government (or business) “dump” products on U.S. markets (capability) and does it have the will to effect such a policy (intent)?

The NCA defines national-level intelligence questions with input from national agencies, the DoD, and individual IC members. The various “INTs” then collect information based on topics and/or countries of concern for dissemination across the IC. While a specific organization may have the lead in providing a final all-source assessment on a particular topic, there is generally no governance precluding other agencies from similarly producing their own assessments. This routinely leads to multiple reports on similar intelligence issues and, while agencies are encouraged to coordinate and collaborate, such activity is inconsistently applied across the IC.

A thorough IC review must address whether the intelligence produced and provided to the NCA adequately answers the questions asked. By what process and standard does the IC measure success? Is it the *amount* of intelligence produced by an IC member or the *relevance* of the intelligence? Are IC agencies providing intelligence in response to specific requirements, or merely generating initiative products for the PDB based on the latest hot topic? Finally, the IC should look to find efficiencies within and between agencies and determine how best to implement them without jeopardizing core missions or support to national security. As the current DNI, James Clapper, often stated when referring to change within the IC, “It’s like changing the tires at the Indy 500 without stopping for a pit stop.”<sup>45</sup>

---

### ***As IC agencies matured based on changing requirements, CIA perhaps experienced the most profound evolution.***

---

As IC agencies matured based on changing requirements, CIA perhaps experienced the most profound evolution. While CIA’s primary function remains “to (collect) intelligence through human sources,” “correlate and evaluate intelligence,” and “provide overall direction” for national collection outside the U.S., the CIA is also empowered to “perform other functions and duties related to intelligence as the President or the DNI may direct.”<sup>46</sup> This latter point is critical; the CIA now conducts many activities heretofore performed by other organizations and entities, thus compounding redundancies and inefficiencies.

After the aborted 1980 attempt to rescue American hostages in Iran, CIA began a robust counterterrorism effort to train foreign proxies in direct military-style action. By the late 1980s and early 1990s CIA was heavily involved in paramilitary operations in Lebanon and Saudi Arabia.<sup>47</sup> This trend continued and, following the 25 November 2001 prison riot in Afghanistan in which a CIA operative was killed,<sup>48</sup> many were surprised to learn CIA now operated its own military-style capabilities alongside DoD’s Joint Special Operations Command (JSOC) forces.

CIA also maintains its own GMI database<sup>49</sup> and operates an Unmanned Aerial Vehicle (UAV) drone program that duplicates military intelligence collection and kinetic strike operations.<sup>50</sup> Following the 2 May 2011 attack on OBL in Pakistan, then-CIA Director Panetta stated the mission was a “Title 50” covert intelligence action employing JSOC forces with the chain of command starting with the President through the CIA Director to the local JSOC commander.<sup>51</sup> CIA has clearly evolved

from primarily serving as the IC's clandestine HUMINT collection steward to maintaining its own paramilitary capability for conducting military-style operations.

NSA has also evolved in both size and scope. In addition to its traditional SIGINT oversight mission, DIRNSA is now dual-hatted as Commander USCYBERCOM. With the exponential growth of the Internet, the world has figuratively shrunk in size and become more susceptible to information theft and systems disruption. With DIRNSA also serving as the head of USCYBERCOM, he has direct capability to enact both cyber network defense (CND) and cyber network attack (CNA), in addition to maintaining oversight of NSA's traditional SIGINT collection and analysis effort.

DIA has similarly undergone significant change. The lead-up to the 2003 invasion of Iraq refocused the IC on GMI, and DIA assumed overall management of the Defense Intelligence and Analysis Program (DIAP).<sup>52</sup> Significantly, DIA invested substantial capability to maintain a robust MIDB and ensure GMI across the IC is as accurate as possible. It modified the previous decision to have CCMDs maintain RESPROD relative to their areas of operation and created the Military Forces Analysis Office to assume RESPROD for a large number of MIDB records.

NIMA became the National Geospatial-Intelligence Agency (NGA) in 2004.<sup>53</sup> As the IC's GEOINT steward, NGA established the National System for GEOINT (NSG) as a venue to coordinate GEOINT production across the IC as well as with international partners. In support of military operations in Afghanistan and Iraq, NGA also instituted an ambitious program to deploy civilian GEOINT analysts to work alongside combat forces.<sup>54</sup> In addition, NGA developed a mobile tactical combat GEOINT capability comprised of teams of two military vehicles complete with tent extensions, internal power generation, and a robust classified communications suite. It later complemented three of these systems with a domestic van version mounted on a fire truck chassis. Finally, NGA extended its traditional GEOINT support role to broader national-level reporting by using GEOINT as the basis for "multi-INT"<sup>55</sup> assessments on myriad national intelligence topics.

## CLARIFYING THE IC LANES IN THE ROAD

As former SECDEF Donald Rumsfeld stated, "You go to war with the army you have, not the army you want or wish to have at a later time."<sup>56</sup> Barring another major armed conflict, combat operations and concomitant intelligence support requirements may wane, and pressure will build for another "peace dividend."<sup>57</sup> Two major paradigm shifts within the IC could result in significant operational and fiscal efficiencies: strengthening DNI oversight of the roles, responsibilities, and intelligence

production of individual IC members, and DoD reassuming larger responsibility for intelligence support to traditional Title 10 operations.<sup>58</sup>

The first step in achieving IC efficiency would be to provide the DNI full budget authority over all IC members. With fiscal constraints as the likely long-term reality, IC members will continue to compete for diminishing resources. Under the current construct, IC agencies engage in discussions of "relevance" to justify greater resources—and compete with each other for input into the PDB so as to be recognized as a major IC contributor during budget season. Full DNI authority to manage the overall IC budget (both NIP and MIP) and the ability to move funds between agencies would mitigate such counterproductive competitive activity.

---

*To avoid future intelligence reporting missteps regarding potential adversarial intent, the State Department's Bureau of Intelligence and Research (INR) could be fully recognized as the premier intelligence organization to provide national-level assessments as they pertain to U.S. foreign and domestic policies.*

---

The DNI ought to manage fully the standard by which to measure individual IC agency success. Rather than relying on individual agencies to determine their intelligence production success, the DNI must develop and maintain a robust process by which to gauge how well IC agencies answer specific questions pertaining to adversarial capability and intent. The DNI must also manage a process by which to determine whether each agency's (and military service's) intelligence production is value-added to the national discourse or merely redundant reporting on the latest hot intelligence topic. With stronger budget authority, the DNI could enforce each IC "INT" steward<sup>59</sup> to remain "in its lane" without concern for budget penalty due to a perceived lack of "relevance" in the eyes of senior policymakers or Congressional overseers. This would reduce IC agencies producing redundant intelligence during crises and mitigate potential reporting inconsistencies.

Under a restructuring based on the initial IC justification, the State Department would be designated as having full responsibility for providing the NCA final all-source assessments on international intent. Since 1947, CIA has maintained almost total exclusivity in gauging other nations' attitudes and actions regarding U.S. foreign policy, often with mixed results. For example, in February 2003 Secretary of State Colin Powell presented the UN a strategic

assessment of Iraq's chemical, biological, and nuclear programs based primarily on a CIA assessment. The assessment relied heavily on a single CIA HUMINT source that was subsequently proven erroneous.<sup>60</sup> The State Department would be better suited to incorporate multiple sources as it has no equity in relying on a particular intelligence discipline.

To avoid future intelligence reporting missteps regarding potential adversarial intent, the State Department's Bureau of Intelligence and Research (INR) could be fully recognized as the premier intelligence organization to provide national-level assessments as they pertain to U.S. foreign and domestic policies. INR would incorporate input from all the "INTs" and serve as the final arbiter in assessing potential adversarial intent. INR analysts would assume primary PDB production responsibility.

---

***The ongoing conflicts in Syria and Iraq against ISIS should be recognized for what they are: an internal insurgency with potential spillover to surrounding countries***

---

FBI must be the lead federal agency responsible for counterterrorism operations worldwide. The NCA would recognize terrorism events as inherently criminal acts to be handled within the U.S. justice system. Through the DNI, the FBI would have primary IC oversight for counterterrorism operations to include activity managed within the NCTC. This would ensure that the criminality of terrorist acts is appropriately prosecuted with assistance from the IC; this distinction would also help mitigate potential *Posse Comitatus*<sup>61</sup> conflicts.

The ongoing conflicts in Syria and Iraq against ISIS should be recognized for what they are: an internal insurgency with potential spillover to surrounding countries (e.g., Lebanon, Jordan, Turkey, and Iran). Citing ISIS as a terrorist organization confuses the issue; terrorism is but one tactic employed by this group to frighten the populace into accepting its political/theological agenda. Treating ISIS as an insurgency would refocus the effort toward a more military and less law enforcement endeavor.

It is essential USCYBERCOM be recognized as a fully independent, national-level intelligence entity from NSA. Alternatively, if the IC agrees that both CND and CNA are viable national-level responses to a cyber attack, USCYBERCOM could be integrated into the DoD Unified Command Plan (UCP) as a separate four-star command. Regardless, the USCYBERCOM Commander must be granted authorities to coordinate all IC-level "CYBERINT"<sup>62</sup>

activities. This would designate the USCYBERCOM Commander as the IC-wide cyber-related functional manager and allow DIRNSA to maintain focus on the SIGINT functional management role.

CIA should refocus on its HUMINT collection functional management role (both covert and overt) and the tradecraft necessary to maintain this capability. As non-state actors increasingly affect world politics, it is imperative the U.S. maintain an ability to infiltrate these groups to discover their capabilities and intentions. CIA remains best suited to provide insight into these groups while avoiding duplication of DoD efforts. CIA should therefore fully manage activities conducted by the Defense Clandestine Service (currently under DIA)<sup>63</sup> to reduce redundancy and potential HUMINT reporting inconsistencies. Recognizing the need to protect HUMINT sources, CIA would be able to focus efforts toward limiting barriers to effective coordination and provide HUMINT-collected GMI information to the DIAP RESPROD organization responsible for military order of battle.

DIA should become the primary national-level all-source military intelligence producer and GMI data repository. With full NIP and MIP oversight, the DNI should also work with the military services to have DIA assume full oversight of each of the individual service intelligence centers.<sup>64</sup> With full GMI responsibility, DIA must avoid reporting on non-GMI political, economic, or informational issues unless a direct GMI link is evident. On the other hand, with full DNI support DIA should call to task those IC members who choose to embark upon GMI reporting without coordination.

---

***The second step in searching for efficiencies would be to initiate a comprehensive review of all IC-level efforts in support of DoD-related Title 10 activity.***

---

NGA should guard against producing all-source intelligence under the umbrella of "multi-INT" and focus on its announced strategy to "put the power of GEOINT in your hands."<sup>65</sup> As both a national-level and combat support agency, NGA must again focus on its GEOINT capabilities at the national level to guard against strategic surprise and continue to provide embedded analytic support to the combatant commands and service intelligence centers<sup>66</sup> as they focus on operational and tactical requirements. NGA should also manage GEOINT tradecraft across the IC, specifically within the military services.

## NATIONAL VS. MILITARY INTELLIGENCE

The second step in searching for efficiencies would be to initiate a comprehensive review of all IC-level efforts in support of DoD-related Title 10 activity. With the appropriate authorities in place, the DNI would be uniquely suited to leverage strategic, operational, and tactical intelligence production across the IC in response to specific military intelligence issues. DNI cognizance over intelligence production at each CCMD JIC would help coordinate its efforts with national-level IC production organizations and reduce potential redundancies. [Editor's Note: The JICs have been upgraded to JIOCs (Joint Intelligence Operations Centers). The bulk of analysts working in these centers are now assigned to DIA.]

The DNI should disapprove CIA activity that resembles military-style kinetic strike operations. The CIA was not designed to resemble the OSS, the latter comprised of military personnel. While intelligence-related Title 50 rules of engagement potentially provide more flexibility in conducting international operations, NCA use of its Title 10 DoD/JSOC forces would ensure clarity of military mission and purpose. CIA should also remain focused on its clandestine HUMINT mission and transfer operating air-breathing overhead collection, specifically its use of drone aircraft to collect full-motion video (FMV),<sup>67</sup> to the CCMDs. CIA-derived HUMINT, along with SIGINT and GEOINT, could still serve to "tip off" military-style direct action.

---

*The concept of competing agencies vying for attention by trying to place an item in the PDB is reminiscent of several individuals trying to get through a door at the same time—an image the IC cannot afford to mimic.*

---

The DNI should direct the military services to assume the requirement to maintain a GEOINT capability in support of combat operations. Each service trains personnel in basic GEOINT; deploying NGA civilians into combat zones is both potentially dangerous and expensive (the NGA Voluntary Deployment Team (NVDT) program provides civilians cash incentives, and civilians receive additional hazardous duty and overtime pay while deployed). NGA should maintain a small cadre of NGA-assigned military personnel (or civilian experts) to deploy tactically as necessary to communicate with the larger GEOINT analytic community and provide reachback continuity as warranted.

## CONCLUSION

With shrinking budgets and changing missions, the IC must review its structure and practices from top to bottom. The desire for "relevance" has caused individual intelligence organizations to develop, follow, or accept missions that, while providing them visibility and a stronger position to argue for resources, has created redundancies the IC can no longer afford. There is no longer latitude for individual agencies to compete for attention in order to garner a larger piece of the NIP or MIP pie, and the DNI should be granted full budgetary authority to provide a tool by which to ensure all members "stay in their lane." Maintaining clear demarcation between Title 50 intelligence collection and Title 10 military operations will also ensure better clarity of purpose. The concept of competing agencies vying for attention by trying to place an item in the PDB is reminiscent of several individuals trying to get through a door at the same time—an image the IC cannot afford to mimic.

### NOTES

<sup>1</sup> The current IC is comprised of the sixteen organizations: CIA, DEA, DHS, DIA, DOE, FBI, INR, NGA, NRO, NSA, Treasury, and intelligence elements within each of the military services (Air Force, Army, Coast Guard, Marine Corps, and Navy).

<sup>2</sup> OCO funding is provided by Congress in response to specific requirements outside the normal funding request process. The POM is the process by which federal organizations outline and justify their funding requests based on forecasted operational requirements within each budget cycle.

<sup>3</sup> Popularly referred to as "chasing the soccer ball" or "chasing the shiny object."

<sup>4</sup> Not be confused with "alternative analysis," welcomed when coordinated and so cited within the reporting.

<sup>5</sup> Renamed the Bureau of Intelligence and Research (INR) in 1957.

<sup>6</sup> Senate Committee on Naval Affairs, 79<sup>th</sup> Congress, Task Force Report on National Security Organization (Eberstadt Report), 22 October 1945.

<sup>7</sup> Harry S. Truman, "Presidential Directive on Coordination of Foreign Intelligence Activities," 22 January 1946.

<sup>8</sup> National Intelligence Authority Directive No. 5, 8 July 1946.

<sup>9</sup> Arthur B. Darling, "The Birth of Central Intelligence," *Studies In Intelligence*, Vol. 10 (Spring 1966).

<sup>10</sup> National Security Act of 1947, Section 102b.

<sup>11</sup> *Ibid.*

<sup>12</sup> *Ibid.*, Section 102e.

<sup>13</sup> *Ibid.*, Title II, Section 201.

<sup>14</sup> George F. Howe, "Early History of NSA," [www.nsa.gov/public\\_info/files/cryptologic\\_spectrum/early\\_history\\_nsa.pdf](http://www.nsa.gov/public_info/files/cryptologic_spectrum/early_history_nsa.pdf).

<sup>15</sup> NSC Intelligence Directive 9, 24 October 1952.

<sup>16</sup> DIA, Historical Research Support Branch, "DIA: 50 Years Committed to Excellence in Defense of the Nation," 2011.

<sup>17</sup> DoD Directive 5105.21, 1 August 1961.

<sup>18</sup> Public Law 81-110, The CIA Act, 20 January 1949.

<sup>19</sup> Public Law 99-433, Goldwater-Nichols Department of Defense Reorganization Act, 1 October 1986.

<sup>20</sup> Established by EO 13354 in August 2004 and later codified by the 2004 Intelligence Reform and Terrorism Prevention Act.



- <sup>21</sup> 2004 Intelligence Reform and Terrorism Prevention Act, Section 2001.
- <sup>22</sup> Conventional Armed Forces in Europe/CFE Treaty, 19 November 1990.
- <sup>23</sup> Andrew Mack, "Why Big Nations Lose Small Wars: The Politics of Asymmetric Warfare," *World Politics*, Vol. 27, Issue 2, January 1975, pp. 175-200.
- <sup>24</sup> The DoD budget declined from \$409 billion in 1990 to \$296 billion in 1998. The overall force structure similarly declined 33 percent, with a 40 percent decline in intelligence personnel. CIA, The 2001 Annual Report of the Intelligence Community, February 2002 (online at [http://www.odci.gov/cia/reports/Ann\\_Rpt\\_2001/intro.html](http://www.odci.gov/cia/reports/Ann_Rpt_2001/intro.html)).
- <sup>25</sup> Ralph Peters, "After the Revolution," *Parameters* (Summer 1995), pp. 7-14.
- <sup>26</sup> As outlined in the National Security Act of 1947.
- <sup>27</sup> U.S. Congress, House of Representatives, 94<sup>th</sup> Congress, 2<sup>nd</sup> Session, Select Committee on Intelligence, "Recommendations of the Final Report of the House Select Committee of Intelligence," HR Report 94-833, dated 11 February 1976.
- <sup>28</sup> PDB responsibility was transferred to the DNI in 2004; in 2010, non-CIA analysts began serving as PDB briefers.
- <sup>29</sup> George Tenet, "DCI Written Statement for the Record Before the National Commission on Terrorism Attacks Against the US," 24 March 2004.
- <sup>30</sup> SECDEF Memorandum, "Strengthening Defense Intelligence," 15 March 1991.
- <sup>31</sup> This later became the Defense Intelligence Analysis Program/DIAP.
- <sup>32</sup> Ronald W. Reagan, "Executive Order 12333," 4 February 1981.
- <sup>33</sup> Lt Gen Michael Hayden, "Statement to the Joint Inquiry of the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence," 17 October 2002.
- <sup>34</sup> DoD Directive 5105.60, "National Imagery and Mapping Agency," 11 October 1996.
- <sup>35</sup> The 9/11 Commission Report, Authorized Edition (New York: W.W. Norton & Co, July 2004), Section 13.1, p. 400.
- <sup>36</sup> *Ibid.*, p. 403.
- <sup>37</sup> *Ibid.*, p. 417.
- <sup>38</sup> *Ibid.*, p. 409.
- <sup>39</sup> James. E. Carter, "EO 12036," dated 24 January 1978.
- <sup>40</sup> Ronald W. Reagan, "EO 12333," dated 4 February 1981.
- <sup>41</sup> The 9/11 Commission Report, p. 409.
- <sup>42</sup> *Ibid.*, p. 411.
- <sup>43</sup> Public Law 108-458, The Intelligence Reform and Terrorism Prevention Act, 17 December 2004.
- <sup>44</sup> *Ibid.*, Section 102.
- <sup>45</sup> As often heard by the author.
- <sup>46</sup> Public Law 108-458, The Intelligence Reform and Terrorism Prevention Act, 17 December 2004, Section 104d.
- <sup>47</sup> "US Antiterrorism Campaign: Policy By Proxy," *The New York Times*, 14 May 1985.
- <sup>48</sup> CIA employee John Micheal Spann was killed during an uprising at Qala-i-Jangi Prison.
- <sup>49</sup> CIA began to maintain separate military order of battle estimates following allegations DoD enemy strength estimates were grossly underestimated prior to the 1968 Tet Offensive. Samuel A. Adams, "Reassessment of US Foreign Policy," transcript of July 1975 Congressional testimony, pp. 155-171.
- <sup>50</sup> The 9/11 Commission Report, pp. 210-211.
- <sup>51</sup> "PBS NewsHour," interview with Leon Panetta, 3 May 2011.
- <sup>52</sup> Per GDIP Directive 006, 31 October 2005, DIA is the functional manager for the Defense Intelligence Analysis Program.
- <sup>53</sup> The 2004 National Defense Authorization Act, 24 November 2003, redesignated NIMA the National Geospatial-Intelligence Agency (NGA).
- <sup>54</sup> NGA Volunteer Deployment Team (NVDT) Program.
- <sup>55</sup> NGA, National System for GEOINT, Basic Doctrine Publication 1-0, September 2006.
- <sup>56</sup> SECDEF Donald Rumsfeld, 8 December 2004 townhall meeting with soldiers in Kuwait, *The Washington Post*, 15 December 2004.
- <sup>57</sup> Support to counterinsurgency operations, such as that against the Islamic Caliphate (ISIS), notwithstanding.
- <sup>58</sup> U.S. Code, Title 10, 10 August 1956, outlines the roles, missions, and responsibilities of the U.S. Armed Forces.
- <sup>59</sup> Intelligence Community Directive/ICD 1, 1 May 2006, identifies functional managers for the HUMINT, SIGINT, MASINT, and GEOINT intelligence disciplines.
- <sup>60</sup> "The Real Story of Curveball: How German Intelligence Helped Justify the US Invasion of Iraq," *Der Spiegel*, March 2008.
- <sup>61</sup> Per 18 U.S. Code, Section 1385, as amended, "The Posse Comitatus Act" precludes federal military forces from engaging in domestic police enforcement operations.
- <sup>62</sup> This would require a minor rewrite of ICD 1.
- <sup>63</sup> "Pentagon Establishes Defense Clandestine Service, new espionage unit," *The Washington Post*, 23 April 2012.
- <sup>64</sup> Current service intelligence centers include Office of Naval Intelligence (ONI), National Air and Space Intelligence Center (NASIC), National Ground Intelligence Center (NGIC), and Marine Corps Intelligence Activity (MCIA). Of note, the Missile and Space Intelligence Center (MSIC) and the National Center for Medical Intelligence (NCMI) are subordinate organizations of DIA.
- <sup>65</sup> <https://www1.nga.mil/Pages/default.aspx>.
- <sup>66</sup> The U.S. Army Intelligence and Security Command (INSCOM) manages the National Ground Intelligence Center (NGIC); the U.S. Air Force maintains the National Air and Space Intelligence Center (NASIC); the U.S. Navy operates the Office of Naval Intelligence (ONI); and the U.S. Marine Corps maintains the Marine Corps Intelligence Activity (MCIA).
- <sup>67</sup> FMV is generally considered a form of GEOINT.

*LTC (USA, Ret) Thomas M. Cooke is a retired Military Intelligence officer whose career included assignments with U.S. Atlantic Command, Supreme Headquarters Allied Powers Europe (SHAPE), Allied Forces Central Europe (AFCENT), and U.S. Joint Forces Command (USJFCOM). He served with the XVIII Airborne Corps as a G2 planner during Operations DESERT SHIELD/STORM. He is a graduate of the U.S. Army Command and General Staff College and holds a BA in Government from St. John's University and an MSSi from National Intelligence University. He currently works for the National Geospatial-Intelligence Agency supporting the Defense Intelligence Agency in Charlottesville, VA.*



---

# The Future of the American Intelligence Establishment

by Dr. William E. Kelly

---

The 21st century so far has provided tremendous challenges to the American intelligence establishment. These challenges will continue and necessitate changes in how the United States meets its responsibility to provide for national security. Although it is difficult to foresee all the changes coming about, it is possible to speculate to some extent what some of them will be in the next decade. Hence, the purpose of this article is to identify probable intelligence changes and to assess their impact on U.S. capabilities to respond to internal and external threats.

The future of the American intelligence establishment will certainly continue to be a current topic for discussion and debate as we move further into this century. Perhaps this is due to past and potential tragedies such as the September 11, 2001, terrorist attacks on the U.S. homeland, Edward Snowden's defection to Russia, and the invasion of the Ukraine by Russia. Lieutenant General Michael Flynn, who directed the Defense Intelligence Agency in 2012-14, warned U.S. officials to prepare for the worst-case scenario following the Snowden leaks. He noted that Snowden caused the United States to lose critical sources of information and that a revamping of the U.S. surveillance network would be an arduous task.<sup>1</sup> Just what "revamping" means is something we do not know at this time. After all, much intelligence work is necessarily clouded in secrecy. However, some changes are coming to the U.S. Intelligence Community and are necessary if we are to provide the most effective protection for the United States. Hence, what follows is a selection of probable changes, keeping in mind that other changes will certainly follow.

There will be greater cooperation between the Intelligence Community (IC) and state and local law enforcement in the future. This may be explained in part because such cooperation increases the chances that harm to this country is more likely to be prevented when various government agencies cooperate to pursue the mutual goal of security. The increased cooperation will also result from the fact that many harmful acts are both criminal and dangerous to our society. For example, money laundering, illegal drug activity, the proliferation of weapons of mass destruction, and gun-running impact both our national security and our criminal laws.<sup>2</sup> Hence, the presence of such activities aptly

demonstrates the need for more cooperation among government entities. One example of such cooperation that might be cited on the local level relates to New York City—a municipal entity that has established a special intelligence unit relating to the prevention of terrorism.<sup>3</sup> This is just one indication of local police getting involved in what is essentially a national responsibility, but such cooperation will probably be increased in this century.

In the future it is also likely that new and more sophisticated sources of information will be present to help the IC. For example, electronic eavesdropping devices are continually being developed which have several advantages. They can easily be hidden, provide a large amount of information, come in a wide variety of types, and often are difficult to uncover. Airborne drones and robots have also more recently been identified as successful sources of information and usage. Drones can be sent on a spying mission without loss of life, often provide a wide scope of information quickly, can cross international borders easily, and may be used to eliminate hostile terrorists or their operational sites.<sup>4</sup> One source notes that the use of drones is spreading because of their economic and strategic advantages. It points out that "more than 30 countries now have drones in service, and the numbers of drones and countries deploying them seem likely to increase."<sup>5</sup> Robots will also become more valuable because they have the increasing potential to perform a host of human tasks such as retrieving terrorist materials, preventing the explosion of various bomb devices, and saving lives.<sup>6</sup>

The countries and parts of the world in the 21st century that will be of major concern for intelligence agencies will not be the same as they were in the prior century. For most of that century, the Soviet Union and Eastern Europe occupied the primary interest of American spy agencies. Although they are still important as evidenced by President Putin's relationship to the Ukraine, U.S. concerns will primarily focus on China, North Korea, and the Middle East as these entities are the major challenges to the role of the U.S. and pose the greatest immediate problems. For example, China is alleged to have a major role in spying within the United States. A number of years ago it was reported that "the FBI has arrested dozens of Chinese on American soil on behalf of the communist regime. According to various reports, there are

close to 500 similar investigations ongoing. The problem is indeed enormous.”<sup>7</sup> In late May 2014, a source was quoted as indicating that “the only computers these days that are safe from Chinese government hackers are computers turned off, unplugged, and thrown in the back seat of your car.”<sup>8</sup> Yet, about a year later in the summer of 2015 the problem seemed to be even bigger when it was announced that a major hacking of the U.S. government’s computer system resulted in every person given a government background check for the last fifteen years being affected by the intrusion. *The New York Times* noted that the hackers stole sensitive information including addresses, health and financial history, social security numbers, and even fingerprints. The attacks were believed to have originated in China.<sup>9</sup> Obviously, having such information is very helpful to any foreign intelligence agency focused on the United States. Yet, it is another reminder of how important it is for the United States to constantly take measures to protect the secrecy of vital information.

Particular countries and certain parts of the world will not be the concerns of the United States alone. Certain groups operating in multiple countries, such as Al Qaida, Hamas, and the Islamic State have been put on a danger list by the United States and thus will receive more attention.<sup>10</sup> These organizations and their leaders will be under enhanced scrutiny by our government regarding their potential for harm to this country.

The 21st century will also see a shift to a broader set of concerns of U.S. intelligence agencies. Traditionally, we have been quite interested in the military capabilities and destructive abilities of those countries which pose a threat to the United States. This concern will and should continue but what constitutes a serious threat to national security will be expanded beyond military force and capabilities. For example, an intelligence report in March 2012 noted “...that countries could use water for political and economic leverage over neighbors and that major facilities like dams and desalination plants could become targets of terrorist attacks.”<sup>11</sup> Another example of the increased concern about new non-military potential threats would be cyberattacks on American assets in one form or another. One source highlights this concern by noting, “Because we already know that other countries have the technology and skills to illegally access secure government databases, it is possible that the entirety of the records on which our economy functions could be erased or stolen. Such an attack would cause mass chaos...”<sup>12</sup>

Considering the recent massive public media attention given to the Snowden disclosures of spying by the United States, it should be no surprise that the subject of U.S. intelligence activity will be quite controversial. More questions will be asked about its efficiency, success, cost, legality, and effect

on privacy. Some will argue that we need to expand our intelligence activities to protect national security. Others will argue that the expansion of intelligence activities is dangerous, especially as it relates to freedom of expression and the intrusion into the personal lives of our citizens. Such negative views followed the enactment of the USA Patriot Act and will probably continue for some time, especially when incidents of what may appear to be illegal spying on U.S. citizens occur. Hence, we can expect criticism in some instances of U.S. intelligence activities by organizations such as the American Civil Liberties Union and other domestic groups concerned with the basic rights of citizens.<sup>13</sup>

In the near future the U.S. Intelligence Community will no doubt see an increase in legislative concern about its activities. This concern will probably result in at least two outcomes. First, new laws will be passed affecting the activities of our intelligence agencies in one form or another. Second, legislative bodies—in particular so called “Congressional watchdog committees”—will be under public pressure to scrutinize U.S. intelligence activities more closely. For example, Senator John McCain (R-AZ) is just one prominent legislator calling for changes which affect the U.S. Intelligence Community. He insisted, “Recent disclosures of these activities and practices have caused grave damage to the United States. They have harmed our relations with friends and allies and harmed our ability to combat threats to the United States. It is more important than ever for Congress to exercise oversight, and where necessary, to enact legislation to address these issues which are vital to American national security. The establishment of a Select Committee is essential to fulfilling this task.”<sup>14</sup>

The rest of the 21st century will likely see the privacy of U.S. citizens being infringed upon by our government. It will not only be easier to access personal information about individuals, but the amount of information sought about a person will be increased. The government will be watching for “links” between citizens and other individuals and groups which pose a threat to the United States. We all know that much information about the private lives of U.S. citizens can now be easily accessed in a number of ways. For example, business companies routinely collect information about the habits and interests of citizens and this information can easily be accessed by our government. The government can also presently obtain information about our reading interests, but it will go further. One source notes that “the Obama administration is drawing up plans to give all U.S. spy agencies full access to a massive database that contains financial data on American citizens in this country...”<sup>15</sup>

It is ironic that, at least in the near future, the U.S. Intelligence Community will not receive as much financial support as in the past, considering the lasting effects of memories of the September 11th terrorist attacks. For example, in fiscal year 2012 the amount of money spent for military intelligence dropped by 10 percent. The budget for national intelligence also dropped from the previous year and the trend will continue.<sup>16</sup> In addition, a source noted, "U.S. intelligence agencies will see a five per cent drop in funding under a proposed 2015 budget..."<sup>17</sup> Just how much impact this trend will have is not known since intelligence costs are spread out among different agencies. In addition, there is a realization that some government agencies not identified as "intelligence agencies" per se could in reality be providing valuable intelligence information.

One source demonstrates how this reduction in government support for intelligence activity may come about: "Savings are achieved by curtailing personnel growth, eliminating legacy capabilities, scaling back operations on lower priority missions, reducing facilities, and implementing new solutions for the delivery of information technology services, as appropriate."<sup>18</sup>

This decrease in federal spending for intelligence activities shows us that advocates of greater intelligence support are going to have to work more diligently to convince our government about the value of their service to this country. Yet, one should keep in mind that government budgets do change and another disaster faced by the United States comparable to the September 11 attacks might increase future spending on intelligence matters.

Intelligence agencies have always relied on dedicated professionals of various types. However, the new employees are probably going to be more specialized in a particular area or will be able to be trained quickly to meet the challenges of their profession. New employees who are well-versed in the latest computer technology will be a necessity since the majority of information is now communicated in this mode. The new employees will also have to be able to "connect the dots" regarding the analysis of the information that comes to them. This will require the ability to see or project a larger picture of a problem facing this country with careful attention given to its causes, possible results, and ways to best react to it.

In the past we have seen universities offering concentrations in Russian Studies and foreign languages. However, we can expect changes in such programs to include more attention to other parts of the world such as Asia, with particular reference to China because of its growing power and to the Middle East because of U.S. interests in that region. In addition, linguists have always been important to intelligence agencies but those who speak

an Asian or Middle Eastern language will be especially sought after, not only by our government but also by private corporations. For example, in 2012 an FBI representative indicated before a Senate Homeland Security and Government Committee that there is a need for individuals who speak Arabic, Chinese, Farsi, and Somali.<sup>19</sup> Considering the scarcity of Americans who have this capability, the recruitment of those who do have it and the teaching of such languages to our citizens to make them effective in using these languages in intelligence work will be a challenging task.

The potential harm that U.S. intelligence agencies will attempt to neutralize in the 21<sup>st</sup> century will be greater than in the past. We all have vivid memories of thousands of our citizens being killed in the September 11 attacks and the destruction of prominent buildings. Yet, the reality of the situation is such that future harm could hurt millions of our citizens, devastate our major metropolitan areas, wreck the national economy, and cause tremendous health problems lasting for generations as a result of biological toxins. Simply put, the stakes are higher today for our intelligence professionals. We have much more to lose than ever before and the potential danger is greater than ever. Hence, we must continually be cognizant of the most effective ways of deterring such calamities. Not only will we see an increase in new technology to bring safety about, but our view of international boundaries as havens for terrorists will change. Our influence will cross these boundaries as demonstrated by the successful elimination of Osama Bin Laden when the United States entered a foreign country (Pakistan) without its formal public consent to find and eliminate him.

Although numerous changes in the IC of the 21<sup>st</sup> century can be expected, one should note that human intelligence assets will continue to be used by our Community. This is quite understandable considering the value of doing so. The right informant in the right place at the right time can save millions of dollars in intelligence costs and often provide unique insights about those who are a threat to us, such as their motivation, future plans, and strengths and weaknesses of their organizations. Perhaps a good example of this in the past was Oleg Penkovsky, a Soviet military officer who provided valuable information to the United States during the Cuban Missile Crisis. One source notes: "Penkovsky is considered one of the most valuable assets in Agency history."<sup>20</sup> Obviously, foreign governments can also be successful in using human assets for their benefit. Both FBI agent Robert Hanssen and CIA employee Aldrich Ames were convicted of helping the Russians.<sup>21</sup> Hence, there will always be a need for human beings as important sources of information. This may be one area that probably will not change for the IC in this century because, as someone once said, "Prostitution is the world's oldest profession," but spying is not far behind and human beings have always been a part of it.



## NOTES

<sup>1</sup> Dollard, Pat, "Putin May Have Access to Top Secret U.S. Intelligence and Battle Plans Thanks to Snowden," <http://patdollard.com/2014/03/putin-may-have-access-to-top-secret-u-s-intelligence-and-battle-plans-thanks-to-american-traitor-snowden/>, accessed April 4, 2014.

<sup>2</sup> IC 21: The Intelligence Community in the 21<sup>st</sup> Century, Staff Study, Permanent Select Committee on Intelligence, House of Representatives, 104th Congress, <http://www.gpo.gov/fdsys/pkg/GPO-IC21/content-detail.html>, accessed April 4, 2014.

<sup>3</sup> Kelly, Ray, Interview with New York City Police Commissioner, "Fighting Terrorism in New York City," <http://www.cbsnews.com/news/fighting-terrorism-in-new-york-city/>, produced by Robert Anderson, Pat Milton, and Nicole Young, accessed April 4, 2014.

<sup>4</sup> "Understanding Drones," [http://fcnl.org/issues/foreign\\_policy/understanding\\_drones/](http://fcnl.org/issues/foreign_policy/understanding_drones/), accessed April 6, 2014. See also Pickler, Nedra, "AP sources: Justice Dept. to disclose drone memo," <http://news.msn.com/us/ap-sources-justice-dept-to-disclose-drone-memo>, accessed May 20, 2015. These sources give one some idea as to important points about the use of drones.

<sup>5</sup> D'Anieri, Paul, *International Politics* (3<sup>rd</sup> edition) (Boston, MA: Cengage Learning, 2014), p. 291 (See "The Attack of the Drones.") See also <http://www.usatoday.com/story/news/politics/2013/02/07/brennan-cia-confirmation-hearing-drones-interrogation/1898347/> —BrennanDefends Intelligence and Drone Policies, accessed April 6, 2014 See also "Drones in the Sky May Might Have Their Eyes on You," <http://www.freep.com/article/20130307/NEWS05/303070197/>, accessed April 6, 2014.

<sup>6</sup> "Tactical & Surveillance Robots for Surveillance, EOD, & SWAT," <http://simulatorsystems.com/tacticalrobotics/>, a description of the possible use of robots for reconnaissance and other activities. Accessed April 4, 2014. See also Lance Winslow, "Spy Robots of the Future," 2002, <http://worldthinktank.net/pdfs/SpyRobotsoftheFuture.pdf>, accessed April 16, 2014.

<sup>7</sup> Newman, Alex, <http://uhrp.org/old/articles/3742/1/Chinese-Spying-in-the-United-States-/index.html>, accessed April 11, 2014.

<sup>8</sup> Williams, Pete, "U.S. Charges China with Cyber-Spying on American Firms," <http://www.nbcnews.com/news/us-news/u-s-charges-china-cyber-spying-american-firms-n108706>, accessed May 20, 2014. See also "Why Is the U.S. Going After Chinese Hackers? Jobs," <http://www.nbcnews.com/#/tech/security/why-u-s-going-after-chinese-hackers-jobs-n109081>, accessed May 19, 2014.

<sup>9</sup> Davis, Julie Hirschfeld, "Hacking of Government Computers Exposed 21.5 Million People," *The New York Times*, July 9, 2015, p. A1.

<sup>10</sup> U.S. Department of State, "Foreign Terrorist Organizations," Bureau of Counterterrorism, September 28, 2012, <http://www.state.gov/j/ct/rls/other/des/123085.htm>, accessed April 11, 2014.

<sup>11</sup> Myers, Steven Lee, "U.S. Intelligence Report Warns of Global Water Tensions," *The New York Times*, March 22, 2012, [http://www.nytimes.com/2012/03/23/world/us-intelligence-report-warns-of-global-water-tensions.html?\\_r=0](http://www.nytimes.com/2012/03/23/world/us-intelligence-report-warns-of-global-water-tensions.html?_r=0), accessed April 11, 2014.

<sup>12</sup> "Cyber-Espionage: The Future of Warfare?" (posted November 17, 2010), <http://www.pctools.com/security-news/cyber-espionage-warfare/>, accessed April 6, 2014.

<sup>13</sup> "Reform the Patriot Act," <http://www.pctools.com/security-news/cyber-espionage-warhttp://www.pctools.com/security-news/>

<http://www.aclu.org/reform-patriot-act>, accessed April 6, 2014.

<sup>14</sup> Statement by Senator John McCain on President Obama's Speech on U.S. Intelligence Activities, <http://www.mccain.senate.gov/public/index.cfm/press-releases?ID=bfb5e379-7c8c-4df5-b9a7-460a0c2dfa38>, accessed April 6, 2014.

<sup>15</sup> Emily Flitter, Stella Dawson, Mark Hosenball, "Exclusive – U.S. To Let Spy Agencies Scour Americans' Finances," <http://www.reuters.com/article/2013/03/13/usa-banks-spying-idINDEE92C0EH20130313>, accessed March 1, 2014.

<sup>16</sup> Pam Benson, CNN, "Intelligence Budget Continues to Drop," <http://security.blogs.cnn.com/category/911/>, accessed April 16, 2014.

<sup>17</sup> "US. Intelligence Budget Declines," <http://www.securityweek.com/us-intelligence-budget-declines>, accessed April 16, 2014.

<sup>18</sup> "National Intelligence Program," article indicating some reasons why the 2014 intelligence budget was lowered. See <http://www.whitehouse.gov/sites/default/files/omb/budget/fy2014/assets/intelligence.pdf>, accessed April 16, 2014.

<sup>19</sup> Tracey A. North, Statement Before Senate Homeland Security and Government Affairs Committee, May 21, 2012, <http://www.fbi.gov/news/testimony/a-national-security-crisis-foreign-language-capabilities-in-the-federal-government>, identifying specific language needs. Accessed April 8, 2014.

<sup>20</sup> "The Capture and Execution of Colonel Penkovsky," <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/colonel-penkovsky.html>, information relating to the capture and execution of Colonel Oleg Penkovsky, who provided valuable information to the United States concerning Soviet military capabilities during the Cuban Missile Crisis. Accessed April 14, 2014.

<sup>21</sup> FBI, "Aldrich Hazen Ames," <http://www.fbi.gov/about-us/history/famous-cases/aldrich-hazen-ames>, contains information about Ames and link to information about Robert Hanssen. Accessed April 16, 2014. See also "The Story of Aldrich Ames and Robert Hanssen," *Cryptography*, <http://marc.info/?l=cryptography&m=110487015422802&w=2>, accessed May 20, 2014.

*Dr. William E. Kelly is a political science professor at Auburn University. He holds a PhD degree from the University of Nebraska. He has received several academic awards, to include one for teaching by the American Political Science Association. He has taught at military bases, community colleges, and a private religious college. He focuses on the areas of American government and criminal justice and also serves as a political science internship coordinator. He has published articles in numerous journals and his review work has appeared in Military Intelligence, Perspectives on Political Science, American Political Science Review, The Journal of Politics, and American Intelligence Journal.*



---

# A Conspiracy Against the Laity:

## Does the Intelligence Community Need an Ethical Code to Become Truly a "Profession"?

by Erik D. Jens

---

### INTRODUCTION

More than a merely semantic distinction divides a “community of professionals” from a “profession.”<sup>1</sup> This essay argues that the Intelligence Community (IC), while undoubtedly the former, is not, by most standard definitions, the latter. This in no way reflects on the high standards of training, character, and integrity necessary for every intelligence professional. Rather, it is a recognition that the traditional professions—law, medicine, and a few others—are entitled to the name by a combination of both highly specialized training common to all within the profession, and a series of historical accidents. To try to stretch the mantle of “the professions” over the IC is to portray the IC as a thing it is not. However, there is, fortunately, a far more tenable and respectable approach: acknowledging members of the IC as a *community of professionals*, in the wider sense of working people everywhere who take a modest pride in mutual solidarity, and in recognition of the importance of competence and integrity in their duties.

George Bernard Shaw famously wrote that “all professions are conspiracies against the laity.”<sup>2</sup> If he was right, then the IC—formal profession or not—should do what it can to at least be a “benevolent” conspiracy, undertaken for the best of purposes: supporting the national security in accordance with law and, yes, high ethical standards.

Whether the IC—profession or not—needs a formal ethical code, and how that code might be conceived and implemented, is a question others have addressed (if not finally resolved) elsewhere.<sup>3</sup> I focus here, rather, on the initial question of how best to define the IC as a coherent entity, and whether it passes basic tests for the traditional professions such as law and medicine.

### WHO IS (AND WHO SHOULD BE) INCLUDED IN THE “INTELLIGENCE COMMUNITY”?

Before discussing whether the IC is a true profession in the traditional sense, we should define what we are talking about. One of several problems with trying to define the IC, especially when the one aim is to formalize its members’ status, is what might be called “the first-grade birthday party problem”: the more people you include, the worse it is to be left out.

Collectors and analysts are obviously doing “core intelligence work”; hence, we might draw the line around them. But what about all the administrative officers, interpreters, computer wizards, and legions of others who support and work alongside the analysts and interrogators? The tighter we draw the definitional circle to define full members of the “intelligence profession,” the more damage we do to the IC’s *esprit de corps*; conversely, the wider the circle, the more attenuated our claim to be a logically and practically unified community.

The obvious solution is simply to define the IC as “everyone formally employed by the sixteen designated intelligence agencies.” That might complicate the process of designing a single ethical code that is relevant to everyone—a problem this author is happy to leave for others to resolve.

### WHY (IF AT ALL) SHOULD WE ATTEMPT TO PROMOTE THE IC TO “PROFESSIONAL” STATUS?

What benefit accrues to the IC from a formal recognition, either among practitioners or the outside world, as a profession? There are at least two possible benefits: First, public service tends to carry with it a measure of pride of position, of one’s earned competence. Recognition of the IC as a formal profession validates that pride and image, in both our eyes and those of the outside world. A second consideration has to do with our motive in approaching this whole question of whether

the IC is a profession. Ethical codes are traditionally associated largely (though not exclusively) with the professions: doctors Do No Harm, academics Cite All Sources, etc. Consequently, publicly characterizing the IC as a profession might lend credibility to an IC-wide ethical code. Perhaps cause and effect work both ways here: creating an IC ethical code might strengthen the IC's case for eventual inclusion among the traditional professions.

What we should avoid is any kind of campaign to formally claim the IC as "one of the professions" without taking concrete steps to bring the IC's structure more into line with the traditional professions. Otherwise, the claim tends to look like mere self-aggrandizement, undermining the real cultural dedication and pride in service that has characterized the IC—however we characterize it—for over half a century.

### **IS THE IC, IN ITS CURRENT FORM, A PROFESSION BY TRADITIONAL STANDARDS?**

**O**f the countless variations on "checklists" for defining professions, I have chosen, for its clarity and applicability to the traditional professions, the six-item list proposed by Professor William Wickenden.<sup>4</sup> Comparing his list to a description of the Intelligence Community is useful for gauging to what extent the IC meets, in broad outline, the standard definition of a profession.

#### **1. *A profession renders services based upon specialized and theoretical knowledge and skill.***

- The IC seems to fit here, with a caveat: the Community consists of dozens of tribes, each with a wholly different knowledge and skill set: case officers, SIGINT analysts, interpreters, lawyers, logistical and financial support personnel, administrative officers, and many others. That said, IC *analysts* generally meet the "theoretical knowledge and skill" test better than do intelligence *collectors*. The former are more apt to live the "life of the mind" in building arguments, comparing evidence, and drafting detailed intelligence assessments; the latter, in contrast, rely more on hands-on training and execution of debriefings, intercept transcription, clandestine source handling, and many other collection-oriented tasks which, while often intellectually and physically challenging, rely less on "theoretical knowledge" than on practical expertise.
- In addition, most traditionally recognized professions have a core of common theory and knowledge which (apart from Community-wide

required security and counterintelligence training) is almost nonexistent in the current IC. The Community is just too fragmented, with too many widely varying skill sets and balkanized institutional knowledge bases depending on the agency and specific job or mission.

#### **2. *A profession maintains extensive education, competence testing, and association restrictions controlling entry into the profession.***

- This "high barriers to entry" test varies widely within the IC. A junior enlisted military analyst or collector may join the Community just after completing boot camp and a short technical course, which often emphasize hands-on skills and "buttonology" over mastery of theoretical frameworks and critical thinking.<sup>1</sup> Civilian analysts, in contrast, are usually more mature and possess a college or graduate degree, but receive only a few months of intelligence analysis-specific training. Case officers are usually commissioned officers, mature and experienced warrant or noncommissioned officers, or fairly mature civilians, with at least a college education; they survive a lengthy and intensive assessment and training pipeline (as opposed to "education"), often for a year or more, to learn the business.<sup>2</sup> In contrast to the above specific experiences required to become collectors or analysts throughout most of the IC, intelligence support personnel may come from almost any background and educational level depending on their function: administration, logistics, human resources, etc. Apart from the need to qualify for a security clearance, almost no common set of entrance standards unifies these and other personnel throughout the Community.
- As for "association restrictions" controlling entry into the IC—yes, it can be hard to break into the intelligence business, but that could be said of carpentry or bartending as well. The total lack of *uniform* education and standards throughout the IC (beyond the universal requirement to qualify for a security clearance) weighs here against considering the IC a profession in the traditional sense.

#### **3. *A profession involves a confidential relationship between a practitioner and a client or an employer.***

- This seems an obvious "yes," for an entire industry based largely on secrecy—but note that most professionals such as doctors, lawyers, and clergy also have direct, confidential relationships with their patients, clients, or parishioners. In contrast, only the most senior IC leaders usually deal directly

---

with IC customers, though of course the duty to protect information falls on all IC members. There is a confidential relationship generally between the whole IC and the entire government, but is this the same as individuals providing confidential services to a consumer, as with doctors, lawyers, and clerics?

- Note that the IC is also unlike other professions in that its sole customer is the government. Only in the most general, attenuated sense is an intelligence report meant for “society”; the IC’s product is directed and consumed by analysts who provide assessments for elected officials. On balance, however, I would argue that the IC does not meet this “confidential relationship” requirement on the level of the individual intelligence officer.

**4. *A profession enjoys a common heritage of knowledge, skill, and status to which professionals are bound to contribute through their individual and collective efforts.***

- This applies generally to subgroups within the IC, such as imagery analysts, interpreters, interrogators, etc., who may all support the same mission but whose actual jobs overlap very little or not at all. Yet, the balkanization of the IC prevents it from satisfying this “common heritage of knowledge and skill” test for a profession.

**5. *A profession has autonomy in how it provides services.***

- The IC is wholly a creature of the government; most of its members have nothing like the professional autonomy enjoyed by doctors, lawyers, and other members of traditional professions.

**6. *A profession has an ethical code.***

- Most IC members belong to the military or to one of the civilian agencies, each of which has an ethical code in place covering all personnel. These codes, however, vary widely in format, intended audience, and applicability to intelligence work specifically. As of now, the IC does not meet this requirement for a *unified* ethos, although this issue is being actively addressed by the National Intelligence University and other institutions.

It therefore seems that most qualities of the traditional professions apply only in part, or with significant caveats, to the IC. I therefore argue that trying to present the IC, either to its own members or to the outside world, as a “profession” in the formally defined sense would be counterproductive. It is too much of a stretch, and the IC is too far-flung and varied, both functionally and

organizationally, to apply the kind of unifying internal controls and discipline possible in, for example, medicine and academia. Most such controls are already exercised quite effectively by the sixteen intelligence agencies over their respective workforces.

## **SO WHAT IS THE IC, IF NOT A PROFESSION?**

If the IC does not qualify as a profession, what else might it be? In one sense, many individual functional tasks within the IC resemble the traditional *guilds*: formal associations of craftsmen with a common set of skills, protected by layers of self-imposed procedures, legal and training hurdles, and other measures intended to insulate their craft from casual usurpation by outsiders.<sup>7</sup> The model of a roughly seven-year apprenticeship, followed by work as a journeyman, with completion of a “master work” marking attainment of master status within the guild, has clear modern parallels in academia, as well as in traditional professions such as medicine, law, and the clergy.

---

*One major feature of the guild system decidedly unlike the modern IC was that the classical guilds were expressly for the sole benefit and protection of their members—they were almost literally, in Shaw’s phrase, “conspiracies against the laity.”*

---

In a sense, the entire early period of modern intelligence work, from the World War II-era Office of Strategic Services through the Cold War, followed this “guild” model fairly closely, but with guilds organized by agency (CIA, FBI, military intelligence services, etc.) rather than by specific occupation or skill set—an inevitable consequence, perhaps, of necessary security practices. It has had the effect, in any case, that analysts throughout the sixteen formal intelligence agencies receive a wide range of training and experiences.

Clandestine human intelligence, with its popular mystique and intensive training process, also follows the general guild structure in its reliance on a combination of formal training and informal mentorship. Newly minted case officers still have much to learn from mentors in the field, from whom they will absorb (one hopes) not only high professional standards but also a healthy pride in their work and willingness to maintain a high barrier to entry into their career field, the better to protect it from the incompetent or unsuitable. All this seems to fit nicely the traditional model



of the medieval guild. Intelligence analysts and others in the IC also go through a period of formal and informal training and gradually increasing responsibility, although analyst training probably varies more throughout the IC than (for example) HUMINT collection training generally.

Another way in which historical guild development parallels the modern IC is in the division of the overall mission into hundreds of discrete tasks, each assumed by a different group of workers. Just as the medieval metal-workers included not only armorers' guilds, but specialty guilds crafting helmets, greaves, polishers, etc., so the modern IC is almost limitless in its division of jobs by both function and organization.<sup>8</sup>

Of course, one major feature of the guild system decidedly unlike the modern IC was that the classical guilds were expressly for the sole benefit and protection of their members—they were almost literally, in Shaw's phrase, "conspiracies against the laity." The few that survived the Industrial Age and evolved into the modern professions did so largely by providing societal benefits: medicine, law, education, and a few others.

## CONCLUSION

It seems that the IC refuses to fit neatly into any characterization more specific than "community." Perhaps asking ourselves if we are truly a "profession" is not quite the right question. Maybe all we really need is a definition of our Community that would facilitate the articulation of a common ethical viewpoint, reflecting our duty to the truth and to our customers and those who elect them.

If this is the case, we already have the right term before us, one with which few would argue: a "community of professionals." Any future measures, such as a unified ethical code for our Community, would only strengthen this sense of teamwork and *esprit de corps* among the professionals of the Intelligence Community.

[Author's Note: All opinions and assessment in this article are those of the author and do not reflect the official positions of the National Intelligence University, the U.S. Department of Defense, or any other branch of the U.S. government.]

## NOTES

<sup>1</sup> Roger Z. George, "Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm," September 10, 2007, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no3/building-a-global-intelligence-paradigm.html> (accessed February 2, 2012).

<sup>2</sup> George Bernard Shaw, *The Doctor's Dilemma*, Act 1 (1906).

<sup>3</sup> Following a January 2012 National Intelligence University symposium addressing the need for an IC ethical code (for which an early draft of this article was created), Director of National Intelligence James Clapper approved the ODNI's issuance of "Principles of Ethics for the Intelligence Community," organized under seven headings: Mission, Truth, Lawfulness, Integrity, Stewardship, Excellence, and Diversity. ODNI website, <https://www.dni.gov/index.php/intelligence-community/principles-of-professional-ethics> (accessed July 11, 2016). Director Clapper, in a September 2014 speech, affirmed his own judgment that the IC is indeed a profession, and that "a professional ethical code [is] necessary because we live in a classified world, where the details of even our oversight are secret, and so it is even more important for us to hold ourselves accountable." ODNI Newsroom website, <https://www.dni.gov/index.php/newsroom/speeches-and-interviews/202-speeches-interviews-2014/1115-remarks-as-delivered-by-the-honorable-james-r-clapper-director-of-national-intelligence-afcea-insa-national-security-and-intelligence-summit> (accessed July 8, 2016). The author provides this background to clarify that this article focuses less on the current official stance toward IC ethical regulation than on a larger discussion of the implications of redefining the IC as a formal profession in the same sense as the traditional professions, and on the implications of casually making claims for the "professional" nature of the IC that could have unintended consequences for the efficiency and morale of our Community.

<sup>4</sup> William Wickenden, *A Professional Guide for Young Engineers*, Engineers' Council for Professional Development, 1967.

<sup>5</sup> U.S. Army recruiting website, <http://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/intelligence-and-combat-support/intelligence-analyst.m.html> (accessed August 26, 2016).

<sup>6</sup> CIA recruiting website for prospective operations officers, <https://www.cia.gov/careers/opportunities/clandestine/core-collector.html> (accessed August 26, 2016).

<sup>7</sup> S.R. Epstein, "Craft Guilds, Apprenticeship, and Technological Change in Preindustrial Europe," *Journal of Economic History*, Vol. 58, No. 3, September 1998, 685.

<sup>8</sup> *New Advent Catholic Encyclopedia*, <http://www.newadvent.org/cathen/07066c.htm> (accessed February 2, 2012).

*Erik D. Jens is a National Intelligence University faculty member and department chair specializing in intelligence collection, ethics, and law. Trained as a lawyer at the University of Michigan, he served for many years as a Russian and Persian Farsi linguist, Army NCO, commissioned officer, and civilian intelligence officer with multiple deployments to Iraq and Afghanistan. He completed a rotational assignment to the Naval Postgraduate School in Monterey, California, where he taught classes while undertaking doctoral research. Erik currently is chair of NIU's Department of Collection and Analysis, and is a frequent and valued contributor to AIJ.*



---

# Mired in Gray:

## Juggling Legality, Lawfulness, and Ethics as an Intelligence Professional

by Dr. (COL, USA, Ret) William C. Spracher

---

[Editor's Note: This article is reprinted and slightly updated from one of the same title appearing in *American Intelligence Journal*, Vol. 25, No. 1, 2007, in order to highlight once again some of the enduring concerns related to intelligence ethics in an issue of *AIJ* dedicated to that subject.]

### INTRODUCTION

At first blush, the title of this piece may seem somewhat awkward, or at least an odd way to categorize intelligence activities. The term "lawfulness" sounds strange to the practitioner's ear, much more attuned to hearing intelligence operations evaluated in terms of their "usefulness," their "effectiveness" or, most often, their "legality." A political scientist might be more comfortable with the word "legitimacy" in place of "lawfulness." Nevertheless, because "lawfulness" is the concept put forth by the eminent social science scholars I cite later, I will stick with that approach and try to illuminate what I mean.

Is there really a difference between "legal" and "lawful"? Can the former be interpreted as the "letter" of the law, while the latter is merely its "spirit"? After all, no rational intelligence professional would consider embarking on an operation that is legal but of virtually no use or, on the contrary, potentially useful but blatantly illegal. I would submit that an intelligence activity which is legal is not necessarily lawful, and that the latter criterion should be carefully weighed before implementing the operation. In turn, an operation that is lawful may not be ethical, but for now I will put that issue aside.<sup>1</sup>

While working at the tactical level as a battalion and brigade S2, the world of intelligence seemed to me distinctly black and white. It was not until I moved to the strategic level and later augmented my practical experience with some international relations theory that I realized everything was not so simple. The role intelligence plays at the national level, specifically in support of foreign policymaking, appears much less clear, though its usefulness never has been in doubt. "Black" and "white" tend to fuse into a broad "gray" area at the national/strategic level, and it is this

area which most concerns me (hence, the "color" of the title). Indeed, at the national level, where intelligence activities have been by far the most controversial and often sensationalized, the interface between intelligence and political decision-makers is a significant issue.

In many situations I have observed or studied over the years, the usefulness of a proposal to employ a certain intelligence technique or tactic seemed to require a temporary waiving of its illegality in return for its long-term benefits. In others, the pernicious illegality of the act clearly overrode any positive gains. Nevertheless, in all too many instances, the trade-off between usefulness and legality was so problematic that appropriate guidance was evident only in hindsight when it was too late to rectify the damage or resulting embarrassment.

### INTELLIGENCE AND PUBLIC ORDER

In this essay I shall borrow ideas from a particular school of thought within the field of international law to suggest an alternative method of considering this problem, for the political decision-maker who must bear responsibility for policy blunders and for the intelligence official who must shoulder the blame for the intelligence failures that appear to be growing in number and severity. The "public order" school was pioneered by the late legal scholar/social science theorist Harold D. Lasswell at Yale University. Trained early as a psychologist, Lasswell later applied psychological/psychoanalytical concepts to the study of politics and international law. He and his disciples began to speak of laws not as static rules but as "norms" transmitted by a process of communication between communicator and target audience. How a norm develops, attended by certain expectations of the involved parties operating from different types of power bases and according to different base values, is set out in a framework called the "world constitutive process."

These academics questioned the practice of determining the lawfulness of certain international actions merely by referring to existent laws, treaties, legal precedents, etc. Instead, they advocated searching to see if a norm regarding such practice either existed or was being crystallized. In

short, they sought an international custom or pattern of behavior which everyone (or at least those who politically counted) had come to expect and deemed right, regardless of specific laws prescribed by individual national legislatures.<sup>2</sup> Such a custom is merely a process of interaction or “interface” among the relevant players. Identifying such a norm was considered much more difficult at the international level than domestically, as I would assert is also true for strategic- versus tactical-level intelligence operations. For example, the act of a brigade S2 or division G2 dispatching an armed reconnaissance patrol in combat seems more “lawful” than the National Security Council approving a covert operation targeted against a country with which the U.S. is not at war. Legal precedent does not help us much here, since both activities are “legal” according to the static rules of the game.

Followers of Lasswell’s approach are guided by two criteria in determining whether an activity is lawful:

- (1) Does it contribute to minimum world order?
- (2) Does it violate the fundamental precepts of human dignity?

Such soul-searching may appear hopelessly utopian and not operationally feasible. I would suggest that, when adapted to the specific situation and understood by all the relevant actors in the decision-making process, these criteria help the players decide whether to authorize a particular intelligence operation. This is especially true when the basic questions (“Is it useful?” and “But is it legal?”) do not permit a logical conclusion to proceed with or suspend an operation.

---

***The criterion of minimum world order involves the goal of maintaining peace and equilibrium in the world by using the least amount of violence possible.***

---

The criterion of *minimum world order* involves the goal of maintaining peace and equilibrium in the world by using the least amount of violence possible. Numerous examples can be cited of operations that qualify on that score. For instance, using so-called “national technical means” for verification of SALT or START accords obviously contributed to world order for many years. Even if Congress for some domestic political reason were to enact a statute outlawing such reconnaissance, the activity, in my opinion, would remain lawful, although technically illegal. Of course, the threshold would be passed if possession of this capability (or the denial of it by Congress) unilaterally increased tensions to the point that a potential for hostilities arose. Then, with the

possibility of violence enhanced, minimum order would no longer be a likely outcome and the activity would become unlawful.

More recently, as highly classified and compartmented material has been more easily declassified and increasingly applied to current world problems, and not just those involving conventional conflict, such organizations as the On-Site Inspection Agency and its successor, the Defense Threat Reduction Agency, have used declassified imagery for the purposes of public diplomacy. Specific cases that come to mind include verification of theater nuclear arms agreements, refinement/delimitation of disputed borders (e.g., the Cenepa River valley/Cordillera del Condor region after the 1995 conflict between Ecuador and Peru), and even assessment of illicit coca eradication efforts where the imagery could be shared with allies (e.g., in Peru and Colombia while the author was serving as a military attaché to those Andean nations during the 1990s).

The second criterion poses more problems for intelligence operations as practiced by the U.S. Here, the protection of human rights comes into play, along with the concomitant implications for interference in other nations’ internal affairs and diplomatic relations by setting up a network of implicit or explicit linkages. This is a perplexing area, especially when realizing that actions aimed at achieving long-term human rights protection might necessitate violence in the short run (witness the current conflicts in Syria, Iraq, and Afghanistan), or those aimed at a peaceful, stable world order might call for a temporary usurpation of human rights (for instance, the ongoing debate over Geneva Convention protections for incarcerated al Qaeda or Islamic State terrorists). However, these are moral and ethical issues the decision-makers themselves must confront, as openly and democratically as possible. To intelligence officials called upon for input, I propose no actions be recommended that obviously violate either condition.

For example, though a planned covert operation could potentially turn around a totalitarian or corrupt regime, leading it toward more democratic methods and fundamental citizens’ rights, the assassination of the dictator to speed the process would not be justified. Such an act would violate the first criterion and therefore be unlawful. The indiscriminate domestic wiretapping of U.S. citizens without their knowledge is also unlawful because, by denying their privacy, the second criterion is violated. Note that I said *indiscriminate domestic wiretapping*, not *deliberate electronic eavesdropping of foreign terrorists* communicating with *domestic* contacts within the U.S. The dispute between certain elements of Congress and former President George W. Bush involving National Security Agency (NSA) activities to counter terrorism shows how easily the waters can be muddied. It should not, however,

be inferred from this discussion that particular categories of intelligence operations are *always* lawful while others are *always* unlawful. Here again, I must stress the dynamic nature of international law, expressed eloquently by legendary political science professor and State/Defense consultant Hans Morgenthau:

Traditional international law and organization derive from a pluralistic, relativistic conception of the state system. Divergent as well as parallel and identical national interests are codified in international law. . . Accommodation and compromise are therefore the necessary political earmarks of such a legal system.<sup>3</sup>

Hence, we must continue to evaluate our intelligence operations and weigh their variables on a case-by-case basis, although the public order criteria do provide a suitable starting point.

### NECESSARY BUT NOT SUFFICIENT – ETHICS ENTERS THE GAME

Now that we have studied the requisites for determining the lawfulness of an intelligence operation, the reader may be wondering if that is sufficient. Of course not. I am merely providing a lowest-common-denominator theoretical framework because I believe the conditions for lawfulness too often have been overlooked in the past. Just because an operation is lawful does not mean it should automatically be implemented. On the other hand, it could be argued I am not being restrictive enough. Why not strive for *optimum* instead of *minimum* world order? Why not shoot for perfection and seek the *ideal*? The late political scientist Robert Dahl cautions us:

What is an optimal system for making decisions is not necessarily what we ordinarily think of as “ideal.” In fact the optimal is almost always different from the ideal. . . The optimal may be a good deal less dramatic than the ideal, but it does recognize that there are many important values in this world and that usually you cannot maximize one value indefinitely without creating astronomical costs to another.<sup>4</sup>

Obviously, within a public order situation, there are countless base values competing for attention and scarce resources that must be considered (desire for security, health, food, etc., or the sorts of commodities reflected by Abraham Maslow’s famous “hierarchy of needs”). A minimal approach which satisfies all of them to some degree, but not at the expense of others, seems most appropriate. The optimal path, and certainly the ideal one, is simply unrealistic and overly optimistic.

Another common method of investigating trade-offs is the so-called “Pareto optimum” (first espoused by Italian sociologist Vilfredo Pareto). This criterion, which states that a decision should be taken if some people’s values will gain and everyone else will remain at least as well off, is normally accepted as a guide for public decision but does not cover cases in which one person’s values must be traded off against another’s. Unfortunately, according to the late John Steinbruner, former Director of the Center for International and Security Studies at the University of Maryland (CISSM) and also former Director of Foreign Policy Studies at the Brookings Institution, most public issues of interest do present such tradeoffs. Information is processed and decisions are ultimately made by individuals; the determination of value ultimately resides with the individual.<sup>5</sup> That is where the ethics of intelligence come into play.

---

*Collegial decision-making is merely a synthesis of individual views, supported by individual inputs from members of the Intelligence Community. Notwithstanding the significance of the individual, however, it should be remembered that there are also group values to be taken into account.*

---

I agree that the game of intelligence analysis, and the subsequent decision or decisions to which it leads, is a highly individualistic one. Collegial decision-making is merely a synthesis of individual views, supported by individual inputs from members of the Intelligence Community. Notwithstanding the significance of the individual, however, it should be remembered that there are also group values to be taken into account. As Roger Hilsman, former Director of the State Department’s Bureau of Intelligence and Research (INR), reminded us, “Organizations have interests of their own that are sometimes more than the sum of the interests of the individual members of the organization.”<sup>6</sup> At any rate, virtually all intelligence officials operate not by Pareto guidelines but by a zero-sum-game approach, i.e., if “they” gain, “we” lose, and vice versa. It is not human nature for an intelligence official to recommend a course of action that will benefit both friendly *and* enemy forces. Indeed, such altruism is not a basic aspect of any intelligence organization anywhere. Nevertheless, a minimum public order regarding intelligence is invaluable in that it implies mutual security for both sides by providing such beneficial services as early warning of hostilities and verification of arms accords.

Once we deem what is lawful by public order considerations, we must further evaluate intelligence operations according to whether they are, in fact, desirable. Many different ways



of doing this have been described. Here are a few questions which should be part of the decision process:

- (1) What are the chances for success and the risks inherent in failure?
- (2) Are there other sources/methods available which are less expensive or risky?
- (3) Even if there are other sources targeted toward the same goal, is repetition or duplication considered beneficial in this case to provide confirming information?
- (4) Is our adversary using similar methods against us, and is *quid pro quo* (something given or received for something else) diplomatically feasible?
- (5) Does the end justify the means?

These questions are valid and should be carefully considered only after the criteria of lawfulness are examined.

Frequently, intelligence officers, operators, and even decision-makers get caught up in purely functional arguments over utility (e.g., whether an operation best reveals intentions or capabilities), cost-effectiveness, or efficiency. The means often are confused with the ends, or one becomes enmeshed in legalistic debates over how to exploit loopholes in executive orders, federal statutes, or regulations.<sup>7</sup> Such efforts are not worthless, for usefulness and legality are important. However, excessive attention to these issues can blind one to the deeper moral and ethical ramifications of intelligence operations and other activities.

Although it may sound otherwise, I am not advocating a crash course in ethics for all intelligence practitioners. There is no scarcity of attention to ethics nowadays, as can be witnessed in classes in any Army officer basic or advanced course, ROTC department, or service academy.<sup>8</sup> Though commendable, such courses are too often programmed in reaction to scandal or bad press. Hence, there tends to be a negative ("Thou shalt not") connotation to these efforts rather than the positive ("Thou shalt") approach I am suggesting in my emphasis on lawfulness. Recent efforts to institutionalize ethics and intelligence and make the study of them more transparent are extremely forward-looking and deserve maximum support from the government, from civilian academia and, hopefully, from the usually skeptical communications media.<sup>9</sup>

Past abuses have prompted a tremendous catharsis of intelligence organizations, epitomized by numerous investigations by the Senate and House Select Committees on Intelligence, the Rockefeller Commission, and increasing inspector general involvement in intelligence planning and oversight. More recently we have witnessed the huge impact of the so-called "9/11 Commission" of 2004 and the "WMD Commission" of 2005 on Intelligence Community

reform and transformation.<sup>10</sup> This trend is generally healthy in that national intelligence agencies no longer have *carte blanche* to do anything they wish. However, the entire investigatory environment has been mostly negative and reactive in outlook, slapping wrists for past misdeeds without providing constructive guidance for the more efficient accomplishment of future tasks.

Naturally, most of the attention has focused on issues producing the greatest sensationalism and public outrage: from alleged drug experiments, assassination plots, and political break-ins in the late 20<sup>th</sup> century to post-9/11 counterterrorist fixes and endless searches for Iraqi weapons of mass destruction in the early 21<sup>st</sup>. Much less notice has been taken of those operations comprising the bulk of intelligence activity, which are typically orchestrated at a much lower level and therefore not under a public lens. There have been, for instance, many unheralded successes by military intelligence elements involved in indications and warning. For better or worse, these often escape both public congratulations and public scrutiny; those that are scrutinized closely often are publicized many years later when operational files are declassified and released. For an incisive discussion of the phenomenon in which bad news about an intelligence failure makes headlines while good news on successes remains in the shadows, see Richard Betts' "Intelligence Warning: Old Problems, New Agendas," in the Spring 1998 edition of the U.S. Army War College journal *Parameters*.

Similarly, some negative thinking has gone into the rewriting of "rules" for the Intelligence Community. In a press conference in September 1978, following several years of intense investigations into domestic intelligence abuses in the 1960s and early 1970s by a variety of Congressional committees and Executive panels, President Carter stressed adherence to ethical rules of the game while lauding the new Foreign Intelligence Surveillance Act (FISA), which he described as one of the most significant legislative initiatives involving intelligence agencies in three decades because of its establishment of the nation's first legislative controls over government-conducted foreign intelligence and surveillance. He added:

The bill also assures intelligence officers who serve our country that their proper activities in this field will be authorized by statute. By providing clear statutory standards, this legislation will help strengthen the ability of our intelligence agencies to deal with foreign espionage and international terrorism.<sup>11</sup>

Since then, the Carter and Reagan administrations, and those that followed, have worked with Congressional oversight committees on additional legislation concerning surveillance of American citizens abroad, to include comprehensive

charters for the various intelligence agencies.<sup>12</sup> Periodic executive orders have also been issued when circumstances warranted further clarification. Yet, no one could have predicted in the 1970s how modern technology (e.g., a plethora of supercomputers, cell phones, BlackBerries, and other miniaturized digital gadgets) would call into question the relatively slow, deliberate procedures called for in the FISA, despite provisions that permit the surveillance to be started and approval gained later after the fact. The sheer mass of high-speed communications today, added to the multiplicity of mobile sources and nodes, have complicated the process considerably.

---

***Without downplaying the importance of such legalistic solutions to prevent abuses, I must assert that one cannot legislate effectiveness, morality, or ethics. These come from the heart and mind of the individual.***

---

Without downplaying the importance of such legalistic solutions to prevent abuses, I must assert that one cannot legislate effectiveness, morality, or ethics. These come from the heart and mind of the individual. His or her interpretation of how an operation can contribute in a positive sense is much more significant than the mere avoidance of criminal acts and legal sanctions. The “rules of the game,” which Harvard professor and former Clinton defense official Graham Allison suggests “stem from the Constitution, statutes, court interpretations, executive orders, conventions, and even culture,” are important, but they are not everything.<sup>13</sup> Or, as his former colleague Morton Halperin qualifies the premise of his book on bureaucratic politics, “the rules do not dominate the process, although they do make a difference to the extent that they structure the game.”<sup>14</sup>

Only a few weeks before his statement on the FISA legislation noted above, President Carter addressed a group of employees at CIA headquarters:

You almost are in the position of being like Caesar’s wife; you have to be even more pure and clean and more decent and more honest than almost any persons who serve in government, because the slightest mistake on your part is highly publicized and greatly magnified, whereas your great achievements and successes quite often are not publicized and are not recognized and they certainly are never exaggerated. There have been too many shocks, too many rapid changes in the past, but the policies that have now been established by Executive Order, by sound

decisions, by cooperation, and in the future by law, will give you a much surer sense of what the future will bring, will liberate you individually, in effect, to make your own beneficial impact in our country be even greater. I know how serious uncertainty is in a person’s life.<sup>15</sup>

An important point to note in this passage is that Carter realized enacting laws takes time; i.e., he was aware of the *future* quality of lawmaking. Rarely is a law placed on the books *a priori*, before an incident giving rise to a need for it occurs. Therefore, we require a guide for the present. “Lawfulness” as I have described it serves as a suitable guide while we wait for “legality” embodied in specific laws and rules to be formulated and legislated. In essence, we strive to adhere to the spirit of American jurisprudence, or what we citizens would consider legal if there was an actual law in place. Individual “ethics” should be part of the equation too, for it helps guide behavior when no clear rules are in place or “when no one is looking,” as is often described as one of its greatest benefits.

---

***Surely, we have all erred on the side of unlawfulness, even with honorable intentions.***

---

Perhaps some of the darkest deeds of the Intelligence Community have been performed in anticipation of future laws proscribing such acts. I have witnessed this penchant for “getting it done while it’s still legal,” if questionable, in such activities as the purging of as many personnel dossiers as possible before an official moratorium on destroying them (which everyone knew was coming) was announced. Destroying the dossiers was perfectly legal; in fact, the so-called “Purge Project” had been ongoing for a couple of years due to the need to reduce the quantity of file holdings, move them to a smaller location, save money, and align the procedures with newly promulgated retention criteria. Still, some observers would question the continued activity knowing that a “cease and desist” order by Congress was in the works. A similar reaction was evident prior to the effective dates of the Freedom of Information and Privacy Acts, which were destined to complicate the gathering and retention of personal data. Needless to say, such actions were not illegal, but their lawfulness and ethical merit can certainly be questioned. I hope this discussion is not interpreted as a self-righteous assertion of discerning right from wrong. Surely, we have all erred on the side of unlawfulness, even with honorable intentions. Instead, my purpose is to arouse the reader to consider

(or devise) guides for action that are more than just technical rules, reactionary moral/ethical standards to satisfy the prying media, or *ex post facto* legislation.

I mentioned earlier how mundane arguments tend to obscure the deeper moral purposes of intelligence operations. Everyday facts of life in intelligence organizations contribute to this shortsightedness. For instance, there are the usual quirks of bureaucratic politics that beset all organizations. The Intelligence Community in particular is plagued by parochialism, which Allison claims is enhanced by the selective information available to organizations.<sup>16</sup> He also suggests that organizational momentum is a problem in the intelligence business since “a program, once undertaken, is not dropped at the point where objective costs outweigh benefits.”<sup>17</sup> This is especially serious in clandestine HUMINT (human resource intelligence), where it can take months to set up an operation and years to gain unfettered access to the target. Naturally, there is organizational inertia against terminating such an effort even when its costs become obvious. Of course, the revitalization of the U.S. government’s HUMINT capability overseas has been much in the news since 9/11 and the beginning of the Global War on Terrorism. Addressing graduating students in August 2005 at the Joint Military Intelligence College (renamed the National Defense Intelligence College in December 2006 and the National Intelligence University in August 2011), Rita Colwell, former head of the National Science Foundation and later a professor at both the University of Maryland and Johns Hopkins University, insisted: “We need your most human intelligence, in which intellect and ethics are fused.”<sup>18</sup> She was likely referring to the rich education the students had experienced, which could be applied in ethical ways where not only the capabilities of our adversaries, but also their intentions, could be gauged.

### THE NATIONAL INTEREST – A VIABLE CONCEPT?

We are all aware of the backlash effect of intelligence failures on both policymakers and intelligence personnel, wherein policy can affect intelligence and vice versa.<sup>19</sup> There is also the preoccupation with doing something “in the national interest.” But the national interest is often highly ambiguous and difficult to define, as is the equally fuzzy concept of “national security.” Intelligence organizations are sometimes hampered by publicity surrounding their involvement in “leaks.” This technique is both good and bad in that it is quite handy for the policymaker who wants to “plant” some information without making it appear deliberate, or wants to send up a trial balloon to assess the consequences, but can have an extremely negative impact, especially on intelligence elements, when the leak is mishandled.<sup>20</sup> Good intentions, e.g., acting in the national interest, can quickly be overcome

by the questionable means used to achieve them. Witness the Valerie Plame situation, for example, which needlessly spun up Congress and the public (the *attentive* public at least), resulted in the indictment of a high-level advisor to the Vice President (for lying in sworn testimony, not for leaking), and in the end fizzled when a retired, and now somewhat discredited, Deputy Secretary of State belatedly confessed he had been the perpetrator of the damaging leak. In the intelligence business, silence is not always golden and plausible denial is not always the best panacea for a sticky dilemma.

Finally, stemming from my previous emphasis on the individual, there is the problem of each of us being led astray by our own biases. One psychologist applying psychological precepts to foreign policy feels the organization itself must institutionalize a procedure that forces officials to try to disprove their own beliefs (i.e., a routine procedure for systematically searching out information that goes against its view of reality).<sup>21</sup> I am skeptical this is workable at the collective level. As Allison and Halperin correctly point out:

Intelligence organizations are not perfect and neutral transmission belts. They notice what their images of the world lead them to think will be important to senior players. They report events and opinions according to established procedures and in ways designed to protect their own organizational interests.<sup>22</sup>

Nevertheless, I am confident that the individual, applying the criteria of lawfulness and his or her own particular ethical code, can begin to overcome personal biases and in some small way benefit the organization. These are just a few of the concerns that can blur the vision of the ablest intelligence professionals and complicate their basic desire to propose operations that are useful, legal and, above all, lawful.

### REFORMING THE SYSTEM

Publicity regarding intelligence abuses in recent years has led to cries for reorganization, new restrictions, purges of leadership, and myriad other “quickie” solutions. For instance, Allison and Peter Szanton, formerly with the Murphy Commission, suggest that the revelations “provide a rare opportunity to rethink and restructure the U.S. intelligence community.”<sup>23</sup> A number of observers over the years have churned out the standard nuts-and-bolts recommendations for structural reform that flood the literature. One example is by the late Ray Cline, former CIA Deputy Director of Intelligence, who suggested revamping the Agency in his mid-1970s book *Secrets, Spies, and Scholars*, written during the heat of the Church and Pike Committee hearings on alleged wrongdoings by selected

members of the Intelligence Community. Another is by a former NSA Director and Army Intelligence chief, the late LTG (USA, Ret) William Odom, in his 2003 book *Fixing Intelligence*.<sup>24</sup> That work preceded the primary piece of legislation driving organizational changes today, which of course was prompted by 9/11, the Intelligence Reform and Terrorism Protection Act of 2004.<sup>25</sup> Nevertheless, would not a rethinking of fundamental values and purposes be more on target?

Likewise, we need more emphasis on the quality of intelligence operations rather than the quantity. Too great a volume of intelligence data has contributed to some of our most blatant failures due to excessive “noise” hindering analysis. Still, we cannot ignore a piece of seemingly meaningless information that might, when pieced together with other data, become extremely valuable. It is a difficult conundrum. Then again, overzealous activity on the international scene can be counterproductive and hazardous to our relations with other nations.<sup>26</sup> Instead, we should seek to cultivate and improve our most useful, reliable, and lawful intelligence sources and discard the rest. This is a tall order, but it can be done with careful evaluation of the sources and assessment of the resulting intelligence. Furthermore, we should manage the sources we retain in an ethical manner, continually reminding ourselves that the end does not justify the means.

## WRAPPING UP—THE INTELLIGENCE INSTRUMENT

In conclusion, what I shall call intelligence “deepening” is sorely needed. The term is used by economists to describe the process whereby capital available to developing countries improves not just in quantity, but in quality, reliability, and per capita distribution. By the same token, a basketball coach is rated by the “depth” of his bench, not its length. In other words, we must strive to better plan, implement, and integrate our intelligence operations, relying in the future on accuracy, feedback, and cross-checking instead of sheer mass, which is both risky and expensive in terms of human capital (though strictly in dollar amounts humans are a bargain when compared to satellites, reconnaissance aircraft, and other technical means).<sup>27</sup> Above all, we should keep in mind that intelligence activity is just one “strategy” toward achieving (and maintaining) world order, to put it in the Lasswellian jargon, as are the other familiar “instruments” of foreign policy—diplomatic, military, economic, and ideological (Latin Americans tend to substitute “psychosocial” for this last one). These tools should be utilized as means to an end, not as ends in themselves, in *lawfully* promoting a stable and cooperative global society.

## NOTES

<sup>1</sup> This article is adapted and updated from a shorter piece written nearly four decades ago when intelligence and ethics were rarely mentioned in the same breath. The period of the mid-1970s was one of considerable breast-beating over legal issues, resulting in many of the intelligence reforms we live and work with today. It was a very anxious and litigious time for the intelligence profession, though many would say it pales in comparison to what we are going through now in the aftermath of September 11, 2001 (hereafter referred to as the “post-9/11” era). See Captain William C. Spracher, “The ‘Lawfulness’ of Intelligence Operations,” *Military Intelligence*, Vol. 5, No. 3, July-September 1979, pp. 11-15.

<sup>2</sup> For a more thorough discussion of the decision process involved in assessing value positions, see Myres S. McDougal, Harold D. Lasswell, and James C. Miller, *The Interpretation of Agreements and World Public Order* (New Haven, CT: Yale University Press, 1977), pp. 55-62. See also McDougal, Lasswell, and Michael Reisman, “The Intelligence Function and World Public Order,” *Temple Law Quarterly*, Vol. 46, 1973, p. 365. The author took an international law course under Professor Reisman while studying international relations at Yale University in 1977-79, a particularly tense period for U.S. foreign affairs.

<sup>3</sup> Hans J. Morgenthau, “Emergent Problems of United States Foreign Policy,” in Karl Deutsch and Stanley Hoffmann (eds.), *The Relevance of International Law* (Garden City, NY: Doubleday, 1971), p. 78.

<sup>4</sup> Robert A. Dahl, *After the Revolution?* (New Haven, CT: Yale University Press, 1970), pp. 48-49.

<sup>5</sup> John D. Steinbruner, *The Cybernetic Theory of Decision* (Princeton, NJ: Princeton University Press, 1974), p. 36. Steinbruner’s paraphrasing of Pareto’s idea is also found on p. 36. A second paperback edition of this book was published with a new preface in 2002 as *The Cybernetic Theory of Decision: New Dimensions of Political Analysis*.

<sup>6</sup> Roger Hilsman, *The Politics of Policy Making in Defense and Foreign Affairs* (New York: Harper and Row, 1971), p. 41.

<sup>7</sup> For the complete text of the January 1978 Executive Order on U.S. Intelligence Activities, see *American Intelligence Journal*, Vol. 1, No. 2, Special Supplement, February 7, 1978.

<sup>8</sup> For example, at the U.S. Military Academy, one of the reasons for redesignating and upgrading an office to departmental status (the Office of Military Psychology and Leadership to the Department of Behavioral Sciences and Leadership) was to place institutional emphasis on the teaching of ethics. See Major Steven Hammond, “The Evolution of an Academic Department: Behavioral Sciences and Leadership,” *Assembly* (published by the USMA Association of Graduates), December 1978, pp. 16-17, 36-37. For a more general and historical discussion of this subject, see “Ethics and the Military Profession,” *Assembly*, March 1979, pp. 12-13, 31-33. An insightful discourse on ethics within the Intelligence Community written from the consumer’s viewpoint is presented by a former Director of Current Intelligence at the Central Intelligence Agency (CIA), who remarks that “to some the mere juxtaposition of ethics and intelligence may appear to be a contradiction in terms. But at heart, intelligence is rooted in the severest of ethical principles: truth telling.” See E. Drexel Godfrey, Jr., “Ethics and Intelligence,” *Foreign Affairs*, April 1978, pp. 624-642.

<sup>9</sup> U.S. Senate, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*,



94<sup>th</sup> Congress, 2<sup>nd</sup> session, April 14, 1976, 7 vols. For brief accounts of specific abuses see, for example, George Riley, "Gray Mail: Corporate Bribery and the CIA," *Multinational Monitor*, Winter 1978-79, p. 13, and "Who Can Be a Paid Spook?" *Time*, January 9, 1978, p. 12.

<sup>10</sup> *The 9/11 Commission Report*, Final Report of the National Commission on Terrorist Attacks upon the United States (New York: W.W. Norton & Company, 2004), and *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Report to the President of the United States (Washington, DC: U.S. Government Printing Office, March 31, 2005).

<sup>11</sup> Jimmy Carter, "Statement Urging Passage of Legislation," in *Selected Statements* (published by the U.S. Air Force as executive agent for DOD), No. 78-9, October 1, 1978.

<sup>12</sup> Nicholas M. Horrock, "Limits Urged to Spying on Americans Overseas," *The New York Times*, February 19, 1979, p. A12.

<sup>13</sup> Graham T. Allison, *Essence of Decision*, 1<sup>st</sup> ed. (Boston: Little, Brown, 1971), p. 170.

<sup>14</sup> Morton H. Halperin, *Bureaucratic Politics and Foreign Policy* (Washington, DC: The Brookings Institution, 1974), p. 115.

<sup>15</sup> Carter, "Remarks to CIA Employees," in *Selected Statements*, No. 78-9, October 1, 1978.

<sup>16</sup> Allison, op. cit., p. 81.

<sup>17</sup> Ibid., p. 91.

<sup>18</sup> Rita Colwell, remarks as commencement speaker at the graduation ceremony of the Joint Military Intelligence College, Washington, DC, August 12, 2005.

<sup>19</sup> For an intriguing look into this problem by a former staff member of the NSC and the Senate Select Committee on Intelligence, see Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics*, October 1978, pp. 61-89. On the specific case of intelligence failures regarding Iran, see Richard Burt, "President Criticizes Intelligence Effort on Crisis Prediction," *The New York Times*, November 23, 1978, pp. A1, A6. Also refer to an editorial in *The Washington Star*, November 28, 1978, with excerpts quoted in "An Intelligence Failure?" *Army Times*, December 18, 1978, p. 15. For criticism of the CIA "bottling up" information crucial to the SALT negotiations, see Burt, "Soviet Reported to Add to Load Missile Can Fire," *The New York Times*, March 14, 1979, pp. A1, A7.

<sup>20</sup> Richard Burt, "Leaks May Be Inevitable in the Ship of State," *The New York Times*, February 18, 1979, p. E4. For another sanguine view see H. Bradford Westerfield, "Congress and Closed Politics in National Security Affairs," *Orbis*, Fall 1966, pp. 737-753.

<sup>21</sup> Joseph de Rivera, *The Psychological Dimension of Foreign Policy* (Columbus, OH: Charles E. Merrill, 1968), p. 61.

<sup>22</sup> Allison and Halperin, "Bureaucratic Politics: A Paradigm and Some Policy Implications," *World Politics*, Spring 1972, p. 59.

<sup>23</sup> Peter Szanton and Graham Allison, "Intelligence: Seizing the Opportunity," *Foreign Policy*, Spring 1976, p. 183. For a critique along the same lines I am pursuing, see comments by George A. Carver, Jr., and Halperin in the same issue. Also see a follow-up by William E. Colby, Walter F. Mondale, Szanton, and Allison, "Reorganizing the CIA: Who and How," *Foreign Policy*, Summer 1976, pp. 53-63.

<sup>24</sup> Ray S. Cline, *Secrets, Spies, and Scholars: Blueprint of the Essential CIA* (1<sup>st</sup> ed.) (Washington, DC: Acropolis Books,

1976), and William E. Odom, *Fixing Intelligence: For a More Secure America* (New Haven, CT: Yale University Press, 2003). More recently, the late General Odom was an adjunct professor at Yale University and senior fellow at the Hudson Institute. See also a review of that book and another on intelligence, Thomas Powers' *Intelligence Wars: American Secret History from Hitler to al-Qaeda*, by Lorraine Adams in "Book World," *The Washington Post*, April 6, 2003, p. 5.

<sup>25</sup> Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, 108<sup>th</sup> Congress, retrieved August 10, 2006, from [http://www.gpoaccess.gov/serialset/creports/intel\\_reform.html](http://www.gpoaccess.gov/serialset/creports/intel_reform.html).

<sup>26</sup> Professor Deutsch warns us that in "world politics, world economies, and world opinion, the very magnitude of our thrust into international affairs has produced some limiting or countervailing responses from the international environment...the essentially unilateral expansion of our power and influence in the world may turn out to be a self-limiting process." Of course, our intelligence effort is part of this overall thrust. See Karl W. Deutsch, *The Analysis of International Relations* (Englewood Cliffs, NJ: Prentice-Hall, 1968), p. 98.

<sup>27</sup> For elaboration of these points see, among others, Colonel Thomas W. Fuller, "Fusion of Intelligence/Operations," *MI Magazine*, July-September 1977, pp. 16-19.

*Dr. William C. Spracher has been a contracted member of the staff and faculty of NIU since 2004. A retired Army colonel, he served over three decades in Armor, Military Intelligence, and the Latin America FAO program. He graduated from the U.S. Military Academy in 1970, holds master's degrees in international relations from Yale University (1979) and military art & science from the U.S. Army Command and General Staff College (1983), and earned a doctorate in higher education administration from George Washington University in 2009. His dissertation dealt with intelligence studies in U.S. civilian colleges and universities. A graduate of the Inter-American Defense College and the Air War College, he taught U.S. government and comparative politics in the USMA Department of Social Sciences and defense planning and intelligence at the Perry Center for Hemispheric Defense Studies, National Defense University. At NIU he has taught courses on Latin America & the Caribbean, peacekeeping & stability operations, globalization, social analysis, and leadership & management in the IC. In the 1990s he served as Army Attaché to Peru and Defense Attaché to Colombia. He is a charter member of NMIA, having joined the former Chesapeake Chapter at Fort Meade, MD, in 1974. Bill has been editor of American Intelligence Journal since 2009 and serves on the NMIA Board of Directors.*



---

# Intelligence Analysts:

## Continuing Education for Enduring Strategic Value

by LTC (USA) Joseph D. Becker

---

### OVERVIEW

In an era of rapidly increasing technical capability where the intelligence focus is often on the modes of collection and tools of analysis rather than the analysts themselves, there is a perception that the role of the analyst is diminishing in importance. This article examines the role and function of the intelligence analyst and discusses the importance, or otherwise, of the analyst to the intelligence system.

The role of the intelligence analyst in the U.S. system of national security has never been more important. Decision-makers of all stripes are bombarded with an unprecedented quantity of data from sources never imagined by their predecessors. Intelligence analysts harness this overwhelming flow of information to provide their customers with “decision advantage,” a term coined in 2008 by the then-Director of National Intelligence, Vice Admiral (USN, Ret) Mike McConnell.<sup>1</sup> However, analysts are not simply computers, striving to process data with ever increasing fidelity until the pace of technology eventually renders their human capabilities obsolete. They have the opportunity to provide a strategic perspective to every aspect of the intelligence cycle and insights that impact national security policy on a level far out of proportion to their individual position or grade. This is precisely what the best intelligence analysts do on a daily basis. Unfortunately, the institutional development of this type of strategic ability is a major challenge for the Intelligence Community (IC). This article argues that intelligence analysts have an active role to play in the development of effective policy and strategy. Furthermore, in order to prepare them to fulfill this role, the IC must develop its strategic thinkers by placing a higher priority on continuing education.

“Improving Strategic Competence: Lessons from 13 Years of War,” a study by the Rand Corporation, examines the relationship between military strategists and policymakers, and it provides useful parallels for evaluating the roles that intelligence analysts play in the formulation of policy and strategy. The Rand study points out that strategy is basically defined as a roadmap

for the realization of policy objectives. Therefore, military leaders look to civilian policymakers to provide their starting point (the “ends”) for the development of their strategic plans. The paradox of this arrangement is that civilian policymakers are often looking to the military to generate options from which to develop their objectives. In addition, policymakers, by nature, are often reticent to limit their own options until absolutely necessary. Consequently, national security policy is often seen as ambiguous, hampering the military’s ability to develop effective strategy until a crisis forces the hand of a President and his administration. On the other hand, military leaders often have been accused of “boxing in” their civilian leaders by providing too narrow a range of military options when they are brought into the planning process. The Rand study concludes that policy and strategy are too interconnected to be conducted separately or in a linear fashion. It is therefore imperative that military leaders understand the policy community, take proactive measures to engage with their civilian counterparts, and participate effectively in the process of policy development.<sup>2</sup>

---

***Analysts are not simply computers, striving to process data with ever increasing fidelity until the pace of technology eventually renders their human capabilities obsolete.***

---

In the case of the U.S. Intelligence Community, the separation between the analytic function and its customers in the planning and policy communities is an important cultural tenet fundamental to the discipline itself. The “politicization of intelligence” is a commonly recognized label that, while often contentious and highly subjective, has been attached to some of the most prominent intelligence failures in U.S. history. Intelligence organizations that lose the ability to conduct objective analysis sacrifice their ability to make credible assessments and reliable predictions.<sup>3</sup> In a military setting, for example, a war game might be reduced to a rhetorical exercise if the intelligence officer wearing the

“red hat” of an enemy commander is overly influenced by the biases of his own unit’s commander or staff. However, as with the findings of the Rand study, strict interpretations of this separation ignore the realities of the policy world and risk stunting the value that intelligence analysts should otherwise provide.

The role of intelligence analysis in the formulation of national security policy is hotly debated, but there is little disagreement over the fact that a strong role exists.

According to the Rand study:

The development of policy objectives, policy options, and strategy requires (1) an accurate characterization of the conflict and the adversary; (2) an understanding of the possible ways of addressing the problem, with the attendant risks and assumptions; and (3) an estimate of means and time required to execute those possible ways. The military is an essential provider of those inputs, as are the Intelligence Community and others, to assist in the framing of objectives and the assessment of options. The dynamic dialogue requires a degree of trust and interaction in an iterative process.<sup>4</sup>

Unfortunately, this dialogue is not always “dynamic.” All too often, intelligence organizations and their analysts will fall back on the need for separation between functions and relegate themselves to a passive role. Sometimes, as pointed out by former National Intelligence University faculty member John Gentry, analysts and managers will display excessive caution in order to avoid the potential for accusations of complicity in failed or controversial policy decisions. They can also deliberately omit important information or analysis that might carry implications unwelcomed by the customers they serve.<sup>5</sup>

On the other hand, these shortcomings can sometimes be attributed to a maturity issue on the part of individual analysts. Instead of framing the issue for their customers and anticipating questions in advance, some analysts allow planning staffs to constrain their focus and then wait to receive specific questions (often known as “requests for information”). Certainly, the relationship with individual decision-makers is built on trust and takes time to develop. However, even young analysts who display initiative and the ability to think critically on the strategic plane will usually demonstrate their value early on.

Compounding the challenges to the IC, policymakers themselves often dip below the strategic levels and delve into tactical and operational matters.<sup>6</sup> This trend has increased in recent years as various details are coming

under greater political scrutiny due to the pervasive influence of the 24-hour news cycle and the wrangling of partisan politics. This means that actions conducted at tactical levels can take on strategic consequences, and it is often difficult to predict which ones will. It also means that issues of little long-term strategic concern are gaining political value and hijacking the attention of policymakers and their staffs. Alternatively, issues with major strategic significance (like the rise of the Islamic State of Iraq and the Levant) can sometimes be overlooked at the policy level until they become too grave to ignore. Roger George, a veteran of the Central Intelligence Agency’s (CIA) Directorate of Intelligence, describes the effect of this phenomenon as “news room syndrome.” He laments specifically that the President’s Daily Brief, a product focused primarily on current intelligence, has become the central focus of much of the CIA’s analytic capacity—to the detriment of long-term strategic assessment.<sup>7</sup>

---

***The tightrope between the intelligence and policy worlds is difficult to walk. The best answers are always situation-dependent...***

---

In order to maximize its value to the policy process, the IC must be capable of identifying strategic implications wherever they arise, satisfying the demands of its customers and yet providing decision-makers with the strategic analysis that they need regardless of whether they have the foresight to ask for it. In any case, the tightrope between the intelligence and policy worlds is difficult to walk. The best answers are always situation-dependent, but analysts with the appropriate skills tend to find the line with remarkable consistency and add strategic value to every process.

The development of an analyst’s strategic thinking skills is not something that happens automatically with the passage of time. In fact, there are institutional forces that pull in the opposite direction. The Gordian knot that binds the intelligence and policy communities may provide opportunities for analysts to increase their value, but it presents dangers as well. Ideas within and among both communities are incestuous. In a world increasingly defined by PowerPoint bullets and sound bites, highly complex issues are often boiled down to oversimplifications that find remarkable staying power. Instead of constantly questioning their assumptions, it is easy for analysts to get lulled into pre-established frameworks that come to be taken as gospel by the organizations in which they operate. This has always been a challenge, and the IC continues to wrestle with

---

this issue. Although examples can be difficult to cite for classification reasons, the below vignette provides an illustration of the point.

Lieutenant General (USMC) Vincent Stewart, the Director of the Defense Intelligence Agency, made the following statement to the House Armed Services Committee in February 2015: "ISIL [the Islamic State of Iraq and the Levant]. . . is a radical ideology that must be countered with a moderate ideology."<sup>8</sup> This short sentence was given as a concise answer to a direct question by a member of Congress. Its brevity was appropriate to the setting. This statement was also nested with policies embraced and directed by President Obama, as confirmed by his recent statements on Islam.<sup>9</sup> Furthermore, this statement represented the distillation of years of evolution in thinking by the military and policy communities with regard to counterterrorism strategy, as reflected in countless publications. Nevertheless, was this assertion, which was made at the highest levels of the IC, actually a relevant or appropriate guiding principle from the standpoint of an intelligence analyst?

---

***The attempts by Hosni Mubarak in Egypt and Bashar al-Assad in Syria to co-opt the Islamic religious establishments of their countries in the years prior to the Arab Spring illustrate just some of the difficulties of state-led attempts to manage the power of belief.***

---

In an academic setting, students might begin an examination of this statement by defining its terms, starting with "ideology" and followed by "radical" and "moderate." They would then proceed to ask a series of questions which would surely include: What makes an ideology compelling (and to whom)? When does a religion become an ideology? Should "moderate Islam" be considered an ideology at all? What historical precedents exist for the defeat of a radical ideology, and what conditions did these victories require? The list would grow for as long as time remained, but it is sufficient to say that this single line of quoted testimony to a Congressional committee contains the power to spawn doctoral dissertations for years to come.

The course of any such discussion would almost certainly reveal that moderate ideologies have little power of appeal over individuals who are not already predisposed to their adoption. Likewise, moderate religions rarely spread like wildfire, change lives, or transform societies. Religions take root specifically because they offer an element of

radicalism that suggests the possibility of changing the status quo. Furthermore, the perception of state affiliation (or approval) tends to reduce the divine quality of a religion, which can significantly damage its appeal. The attempts by Hosni Mubarak in Egypt and Bashar al-Assad in Syria to co-opt the Islamic religious establishments of their countries in the years prior to the Arab Spring illustrate just some of the difficulties of state-led attempts to manage the power of belief. None of this means that the Obama administration's current approach to tackling radical Islam is doomed to fail, but it serves to illustrate that an established maxim, dutifully stated by the director of a U.S. intelligence agency, is entirely questionable in value.

This is certainly not the first time that academic questions have been raised over this particular assertion. Debates over the best way to combat Islamist extremism have raged since the attacks of September 11, 2001. The concept that the fight against terrorism is primarily a war of competing ideologies has gathered momentum over time and gained ascendancy within the military and policy communities. There are solid underpinnings to this theory, but there are also significant practical and intellectual challenges that have yet to be addressed in turning this into a winning strategy. In a fashion entirely characteristic of both the military and the Washington policy community, this incredibly complex and contentious issue has been reduced to a 5-second sound bite. If intelligence analysts fall prey to this pattern of oversimplification, they risk misinterpreting the data which they are presented and missing out on important insights that might increase their strategic value.

How can the IC equip its analysts to avoid the pitfalls presented by the constant barrage of policy rhetoric so they can maximize their strategic value? One of the most important methods is through continuing education, and particularly education with a strong theoretical grounding. "Theory" is a word much maligned in the fast-paced and high-pressure world of national security. Readers will find little direct reference to theoretical terms in the vast majority of intelligence products. However, it is this tool which helps analysts apply their skills at a higher level. The examination, synthesis, application, and critique of various theories allow analysts not only to model their world but to objectively evaluate the models they have created, both consciously and unconsciously. Understanding theory helps analysts to ask the right questions. Asking the right questions helps them make better assumptions. When they combine solid assumptions with an understanding of historical factors, they perform better analysis and make more accurate predictions. Theory may not shine explicitly through intelligence products, but its underlying influences



---

pervade, for better or worse. As political scientist Joseph S. Nye, Jr., has written, "In practice, theory is unavoidable."<sup>10</sup> Therefore, how is the IC doing in regard to this type of continuing education?

When young analysts are hired into the IC, often fresh from their undergraduate or graduate education, they arrive full of energy and ideas. They are coming from an environment where they were rewarded for intellectual curiosity, and their opinions were given value. Their introduction to the workplace is often a rude awakening as they are subjected to a litany of institutional practices and procedures. They are trained and molded in the process and methodology germane to their particular lane of intelligence analysis and production. Because young analysts lack experience, their opinions and ideas are quickly discounted and often filtered out of final products. This is a sad state of affairs for the Community's new members, but the process is both a fact of life and an absolute necessity for their organization.

---

***Intelligence organizations, especially on the civilian side, tend to place little value on continuing education for their analysts.***

---

Intelligence organizations have limited time and resources with which to respond to a world of threats and policy concerns. Managers are compelled to allocate and utilize their analytic resources as efficiently as possible. "Out-of-the-box" thinking can be an expensive commodity for any type of organization. In the IC, for every wild success achieved, there are often countless hours wasted considering low-probability events that never materialize. It is therefore natural that managers focus and direct their junior analysts for the greatest probability of success. However, these junior analysts do not stay young and inexperienced for long. The point at which they begin to reach professional maturity is when continuing education is especially important to the development of strategic thinking skills. It is also the point at which analysts are at the greatest risk of becoming institutionalized by their organizations.

Intelligence organizations, especially on the civilian side, tend to place little value on continuing education for their analysts. Whenever possible, they hire individuals at exactly the level of education and skill they are seeking, and they are reluctant to devote resources toward further development. Analysts routinely undergo training for job-specific skills that are unique to the IC, but training and education are not the same thing. Although the line between the two is often murky, Professor Peter Rickman provides a generally accepted guideline:

Training is about practice, about skill, about learning how to do things. Education is about fostering the mind, by encouraging it to think independently and introducing it to knowledge of the physical and cultural world. It's about theory, understanding and a sense of values.<sup>11</sup>

Educational activity removes analysts from their element and deliberately directs their focus outside the scope of their normal duties or expertise to foster critical thinking skills and a broader strategic understanding.

Given the demands placed upon the IC and the resource constraints under which it operates, it is not surprising that its component organizations are loathe to dedicate money or man-hours to any venture that does not provide an immediate return on the investment. Educational opportunities may or may not produce a measurable improvement in the quality of an analyst's day-to-day tasks. Perhaps more importantly, though, existing personnel management systems make it difficult for civilian organizations to afford opportunities for their analysts. Unlike the military, which programs educational opportunities into career timelines and personnel assignment schedules, most intelligence organizations will sacrifice capacity if a specific analyst is away from his or her desk too long. Seasoned, mid-career analysts in particular are at a point where they are increasing in utility to their organizations. Training may be considered a necessity, but education is not. Lastly, in some cases, education may afford the analyst the opportunity to compete for higher positions or even jump ship to a different agency. Although this might be a net benefit to the Community as a whole, it could be a tough sell to an individual manager faced with the prospect of losing his/her analyst's services.

What should education look like, in practice, for a mid-career (or even more senior) analyst? Is theory a magic bullet to sharpen minds within the analytic community? If this were the case, the answer would be simple. In a manner typical of government bureaucracies, intelligence organizations could form working groups or appoint a new deputy to examine the problem. This process might continue its course until the community had produced a suitable "dummies guide to theory" for its analysts and mandated its incorporation into all training programs and briefing formats. However, if the value of theoretical conception was this easy to isolate, then it is unlikely that the term would have fallen from grace in the first place.

The true value of theory is in educating analysts and sharpening their cognitive abilities. There is no "CliffsNotes" method for accomplishing this. Analysts are better off internalizing, testing, and applying a few

theories than building a cursory knowledge of many. For best effect, they need the opportunity to step out of their daily environment and examine difficult problems through new and different paradigms. They need the challenge that comes from presenting and defending their ideas to peers and knowledgeable instructors. Academics have also argued ad nauseam over which disciplines and associated theories are the most important for educating an intelligence analyst. Most options presented have merit in their own context, and the debate ultimately devolves to a question of who has the best “kung fu.” The point is that, regardless of which disciplines they study, all analysts should have the opportunity to have their existing mental models challenged at regular intervals throughout their careers and be afforded the opportunity to expand their horizons.

---

***All analysts should have the opportunity to have their existing mental models challenged at regular intervals throughout their careers and be afforded the opportunity to expand their horizons.***

---

The younger generations that are filling the analyst ranks today have been encouraged by popular culture to “question everything.” Unfortunately, the same popular culture provides few, if any, of the tools necessary to make valid assessments or comparisons, leaving individuals as susceptible as ever to the influence of misinformation, shallow slogans, and clever marketing. The IC fares better in this regard, hiring bright and promising individuals with strong academic backgrounds, and these individuals have an important role in the formulation of both policy and strategy. However, the Community does far less well in developing these individuals over time. The inevitable and necessary overlap between the intelligence and policy communities exposes analysts to an incessant barrage of agendas and institutional rhetoric that grind against the sharp edge of an analyst’s abilities for independent thought. The only way for the Intelligence Community to build and sustain a corps of highly competent, value-adding analysts over time is by making high-quality educational opportunities a priority throughout the course of these individuals’ careers. This type of analyst will never diminish in importance, regardless of the advance of technology.

#### NOTES

<sup>1</sup> Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 6<sup>th</sup> ed. (Thousand Oaks, CA: CQ Press, 2015), 258.

<sup>2</sup> Linda Robinson, Paul Miller, John Gordon IV, Jeffrey Decker, Michael Schwille, and Raphael Cohen, “Improving Strategic

Competence: Lessons from 13 Years of War” (Santa Monica, CA: Rand Corporation, 2014), 32-36, 42.

<sup>3</sup> Lowenthal, 189-192.

<sup>4</sup> Robinson et al., 34.

<sup>5</sup> John A. Gentry, “Managers of Analysts: The Other Half of Intelligence Analysis,” *Intelligence and National Security*, published online (October 2, 2014): 17-19, <http://dx.doi.org/10.1080/02684527.2014.961244> (accessed March 27, 2015).

<sup>6</sup> Robinson et al., 36.

<sup>7</sup> Robert Z. George, “Reflections on CIA Analysis: Is It Finished?” *Intelligence and National Security* 26, no. 1 (February 2011): 74-77.

<sup>8</sup> U.S. House Armed Services Committee, *Worldwide Threats*, 114<sup>th</sup> Congress, 1<sup>st</sup> Sess., February 3, 2015, <https://www.youtube.com/watch?v=y5PGdmN40nA> (accessed March 6, 2015).

<sup>9</sup> Byron Tau, “Obama: U.S., West at War With Extremists, Not Muslims,” *The Wall Street Journal*, February 18, 2015, <http://www.wsj.com/articles/obama-were-not-at-war-with-islam-1424296897> (accessed March 6, 2015).

<sup>10</sup> James N. Goldgeier, “The Academic and Policy Worlds,” in *Security Studies: An Introduction*, ed. Paul D. Williams (London: Routledge, 2013), 556.

<sup>11</sup> Peter Rickman, “Education Versus Training,” *Philosophy Now*, No. 47, 2004, [https://philosophynow.org/issues/47/Education\\_versus\\_Training](https://philosophynow.org/issues/47/Education_versus_Training) (accessed March 6, 2015).

[Editor’s Note: This article was adapted from LTC Becker’s award-winning essay submitted to the International Association for Intelligence Education. In 2015, his outstanding work earned him first place in IAFIE’s annual intelligence essay contest in the “professional” category.]

*Lieutenant Colonel Joseph D. Becker is a U.S. Army Strategic Intelligence Officer. He is currently detailed to the National Counterterrorism Center as a strategic planner. His broad range of intelligence and special operations assignments include service as chair of the Military Strategy Department at the National Intelligence University, where he continues as an adjunct faculty member. His teaching responsibilities have included such courses as Intelligence & the Global Strategic Environment, Social Analysis & the Spectrum of Conflict, Asymmetric Warfare, and a foundational elective on Iran. Joe holds a BS degree in Industrial and Systems Engineering from Virginia Tech, an MBA from Webster University, and an MSSI from the National Defense Intelligence College (now NIU).*



# Lessons on Cyber Security: A NASA Case Study

by Dr. Joshua Tallis

---

On February 1, 2003, the Space Shuttle *Columbia* broke into pieces above Texas and Louisiana upon reentry. All seven astronauts on board were killed. At first blush, this tragedy seems to have very little bearing on those outside of the aerospace industry. Indeed, the first several chapters of the ensuing Columbia Accident Investigation Board report deal very specifically with the technical components of the disaster. A piece of foam insulation used to keep condensation from forming on the Shuttle's external fuel tank broke off upon launch and caused a gash in the craft's left wing. This gash was suffused with heated gas during reentry, ultimately destabilizing the wing and eventually the ship itself. Yet, the report goes on to note that this technical failure is only the most visible component of a much longer chain of complicity. It is in this deep analysis that we see an important lesson for understanding cybersecurity today.

The questions asked after every major hacking incident are the same. Who did this? How did they get into the system? Whose job was it to stop them? In scope these are similar to the questions asked regarding the foam coating on *Columbia* after the accident. Who applied the coating? Who inspected the material? Who was supposed to manage this process? Yet, as the board's report notes, these questions only take us so far:

Many accident investigations make the same mistake in defining causes. They identify the widget that broke or mal-functioned, then locate the person most closely connected with the technical failure: the engineer who miscalculated an analysis, the operator who missed signals or pulled the wrong switches, the supervisor who failed to listen, or the manager who made bad decisions. When causal chains are limited to technical flaws and individual failures, the ensuing responses aimed at preventing a similar event in the future are equally limited: they aim to fix the technical problem and replace or retrain the individual responsible (Report, p. 177).

Buried deeper in the *Columbia* review board's report come sections on the institutional culture of the National Aeronautics and Space Administration (NASA). It is here that we see just how deeply the fissures of the accident

reached. Managers and administrators began, ever so slowly, to accept small bits of risk as routine. Foam insulation broke off from the external tank on virtually every flight. This, in turn, almost always caused some degree of damage to the craft. Yet, since no accident had occurred, such incidents were incorporated into the conception of Shuttle operations as normal events. More broadly, operators began to conceive of the Shuttle as an operational ship instead of more accurately viewing it as a developmental craft. The results of such institutional conceptual framings compounded, over time becoming immense, even overriding. The board felt that merely identifying culpable key policymakers would not reverse such institutional bias. No matter who was making the decisions, the weight of organizational culture would have a deep and predictable influence on the agency's actions.

This is reminiscent of wider research on organizational culture, which has become an important component of work on security. John Nagl, for instance, reaches into such a bank of research for his work on obstacles to institutional learning in the U.S. Army during the Vietnam War (Nagl, 2002). The board's report similarly cites a common element of organizational research: "People's actions are influenced by the organizations in which they work, shaping their choices in directions that even they may not realize" (Report, p. 170). NASA's organizational influence, as indicated above, was shaped by years of slowly integrating flawed assessments of risk mitigation. Each individual slightly erroneous assessment was then further magnified by the familiar strains of budget and time. Invariably, "When a program agrees to spend less money or accelerate a schedule beyond what the engineers and program managers think is reasonable, a small amount of overall risk is added. These little pieces of risk add up until managers are no longer aware of the total program risk, and are, in fact, gambling. Little by little, NASA was accepting more and more risk in order to stay on schedule" (Report, p. 139). Hence, we arrive at the paramount concern in the evolving popular conception of cybersecurity: the slow acceptance of risk.

In a recent interview on Public Radio International's *Science Friday* program, author and security consultant Marc Goodman was asked whether the public needs some kind of high-profile incident to help jolt an understanding of the

magnitude of cyber threats. He keenly noted that such incidents in fact occur every day. Sony Pictures Entertainment is attacked by North Korean-sponsored hackers. The mega-retail store Target has tens of millions of customer credit card numbers stolen during the holiday shopping season. Anthem, one of the nation's largest health insurance companies, has records stolen belonging to tens of millions of policyholders and personnel. Hackers manipulating the Associated Press' Twitter account once sent the stock market into a three-minute tumble worth over \$100 billion in short-term losses. The average Fortune 500 company, which is attacked daily, goes an average of approximately seven months before detecting breaches in its systems, according to Goodman. Energy infrastructure is vulnerable to catastrophic damage from actors sponsored by China or Russia. Yet, in the public sphere, it all just seems to roll off. After the sensationalized headlines, cyber recedes into the background until another event gushes to the fore. By all accounts, any one of these or countless other events should have broken the dam and, as Goodman puts it, inspired a cybersecurity Manhattan project. Therefore, why has it not done so?

The answer may be buried in the Columbia Accident Investigation Board's report. The same phenomenon that built incremental changes in perceived risk into a life-threatening gamble is perhaps now keeping the government, the public, and business sectors from addressing the catastrophic level of risk to which they daily expose themselves on networked systems. In an ironic way, it may be the very visibility of the issue, the constant simmer of weekly headlines, that is part of the problem. In a discussion with CNN's Fareed Zakaria on the *Global Public Square* program, former counterterrorism and cybersecurity czar Richard Clarke alluded to much the same phenomenon, noting that cyber attacks are characterized as a "drip, drip, drip kind of problem, not one major event" that galvanizes action. When we as a society come to see cyber threats as the new normal, we allow incremental changes in risk to compound imperceptibly but alarmingly, without taking adequate heed. NASA's engineers slowly began to internalize foam displacement and damage to the spacecraft as normal and acceptable because of its repeated occurrence. The enduring challenges of shrinking budgets and deadline pressures pushed this risk even further. The result was an operating environment that vastly underestimated the true dangers of space flight. Just the same, our incremental exposure to cybersecurity breaches has failed to raise the alarm to a suitable decibel in some sectors because of a prolonged, tepid exposure to the issue.

None of this is to say that experts in and out of government do not take cybersecurity seriously. However, NASA also took safety seriously. The concern is that our operating environment, the greater climate in which businesses and

government act, conditions those in positions of authority to misread the indicators. Overcoming this ingrained downsizing of the threat can be done only with great awareness of our blind spots. This was among the board's most pressing lessons for NASA. It recognized that engineers would not likely repeat their mistake, that the significance of damage caused by foam debris would become a point of significant scrutiny going forward. Yet, without a comprehensive shift in the culture of risk internalization, the review board believed still more tragedies could occur in the future.

We are presented with an opportunity to learn from this case in the cyber domain. Instead of focusing exclusively on the technical minutia in the wake of hacking scandals, we need to address the very culture in which they take place. Only by tackling society's chronic misdiagnosis of the severity of the threat will we begin to consider mustering the tools and resources necessary to combat it.

[Author's Note: The views expressed in this article do not necessarily reflect those of my university or my employer.]

## References

*Columbia Accident Investigation Board Report*, Volume 1 (Washington, DC: 2003).

"Future Crimes: The Next Generation of Security Threats," *Science Friday*, Public Radio International, February 27, 2015, <http://www.sciencefriday.com/segment/02/27/2015/future-crimes-the-next-generation-of-security-threats.html>.

John Nagl, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Chicago: The University of Chicago Press, 2002).

*Dr. Joshua Tallis is a research specialist for a nonprofit research and analysis organization located in Arlington, VA. He recently graduated from the University of St. Andrews in Scotland, where he earned a PhD in International Relations from the Centre for the Study of Terrorism and Political Violence. His dissertation dealt with maritime security. Earlier he earned a BA in Middle East Studies from the Elliott School of International Affairs, George Washington University. Josh has written on both aerospace and defense matters in Strategic Studies Quarterly, SpaceflightInsider.com, and the Journal of Counterterrorism and Homeland Security International.*





# Can Traits of a Successful Military Commander Be Those of a Good Intelligence Director?

## A Look at Field Marshal Erich von Manstein: Extraordinary Military Leader

by Dr. Kenneth J. Campbell

---

### INTRODUCTION

The objective of this article is to delineate the traits which an intelligence leader should have by reference to Feldmarschall (Field Marshal) Erich von Manstein, who along with Field Marshal Erwin Rommel and General George Patton represents the very best in military leadership. The exploration of military leadership can be a guide to what is needed among intelligence leaders, a theme which can be most clearly developed through examination of the achievements of men such as Manstein. First, I will relate Manstein's background which placed him in a position of leadership in the German Army in World War II. Second, I will highlight his battlefield successes and the personality characteristics which facilitated them. Finally, Manstein's traits will be related to what is required of an intelligence leader.

### EARLY LIFE

Erich von Lewinski was born on 14 November 1887, the tenth son of his father, retired General Eduard von Lewinski, and the fifth child of his mother Helene (Eduard's second wife). Helene's sister, Hedwig, was barren. Helene gave Erich to her sister, whose four brothers were officers and who was married to an officer, Georg von Manstein. They maintained a stable home and often permitted Erich to visit his natural parents.

At the age of 12, Erich, surrounded by military officers, entered the Royal Prussian Cadet Corps. For the first two years of his military education he was sent to the junior cadet school at Ploen where he was taught the Prussian virtues of duty, honor, and obedience. At age 14 he went to Gross-Lichterfelde in Berlin, a royal institution which also trained princes, and was reputed to be comparable to West Point. This is where Germany's future generals, such as Gerd von Runstedt and Heinz Guderian, were trained. Although life as a cadet was mentally and physically hard, Erich was determined not to fall behind his comrades. This institution inculcated self-control and the mastery of

fear, both of which Erich thoroughly learned as shown in his leadership in later years. He was also a page at the royal court of Kaiser Wilhelm II. Upon completion of his studies in 1906, Erich obtained the *Abitur*, which qualified him for entry into the university, but subsequently joined the prestigious 3rd Prussian Foot Guards as an ensign in 1906.

Erich was promoted to second lieutenant (*Leutnant*) in January 1907. Receiving extended leave, he traveled widely in Germany, the Baltics, Turkey, Greece, and Italy, but continued to serve in the 3rd Foot Guards. His talent as an officer was recognized, enabling him to enter the War Academy (*Kriegsakademie*) in 1913, where he began a 3-year course in operational and tactical problems. The General Staff of the War Academy prepared timetables for mobilization, studied past wars for development of doctrine, developed war games, and conducted staff rides. Manstein's general staff training was interrupted when World War I broke out in 1914, and he was subsequently sent to a combat unit. However, his military education resumed after the war ended. He read extensively, educating himself, as shown by his personal library.

On 19 June 1914 Manstein was promoted to first lieutenant (*Oberleutnant*), becoming Regimental Adjutant, 2nd Garde-Reserve-Infantry. His first action on the Western Front was the storming of the Belgian fortress at Namur with the help of a 420-mm siege gun, "Big Bertha," in August 1914. The Guards Reserve Division was next sent to the Eastern Front to stop the Russian invasion of East Prussia, at which time Manstein fought in the Battle of Masurian Lakes. When Manstein next fought in Poland, he was severely wounded in the left shoulder and knee, prompting his colonel to say, "That'll teach you."<sup>1</sup> This setback required him to spend six months in the hospital. For his part in the fighting he received the Iron Cross Second Class for bravery.

In 1915 Manstein joined the staff of the Tenth Army on the Eastern Front where he learned the problems of coordinating operations at the army level. He was

promoted to captain (*Hauptmann*) on 24 July 1915. In 1916 he was once more on the Western Front where he witnessed the horrors of the Battle of Verdun, its senseless slaughter, and afterward the bloody Battle of the Somme (July-November 1916). On 4 May 1918 he became operations officer of the 213th Division (Assault) on the Western Front, where, in contrast to the German method of holding on to every yard, the flexible method was utilized whereby the defender gave ground until the attacker was exhausted and then attacked. This was the essence of Manstein's defense in the Soviet Union in World War II. On 1 October 1917 Captain Manstein returned to the Eastern Front again where he was appointed to serve under the Chief of Staff of the 4th Cavalry Division. On 4 May 1918 he was transferred to the 213rd Infantry Division, a unit where he was trained in "storm troop" tactics.

By August 1918 the Allies were advancing across the Western Front, as the German Army disintegrated. With a naval mutiny and increasing unrest at home, the Germans asked for peace terms. The Kaiser (King), the embodiment of honor and dedication in Germany, renounced his throne on 9 November 1918, and this was followed by establishment of the Weimar Republic. Manstein was supposed to switch his allegiance from a king to a concept, the republic, which explains why he remained a monarchist.

### INTERWAR YEARS

Manstein had earned the Iron Cross (First Class) and Iron Cross (Second Class), as well as the Knight's Cross, during World War I. He had spent the conflict at the army, corps, and division levels, which gave him the experience of seeing the problems of handling large groups of troops. When General Hans von Seeckt became Chief of Army Command in 1919, he began a massive study of the war from which came forth the doctrine of mobility, which was of prime importance to Manstein and other officers in World War II. In 1919 Manstein became part of the group which reduced the size of the Army to 100,000 in accordance with the Treaty of Versailles.

In 1920 at age 31 Erich Manstein married Jutta-Sibylle von Loesch, who proved to be an asset to her husband. He claimed that she was a "mile" barrier against his egotism. In 1921 Manstein was appointed commander of the Sixth Company in the new Reichswehr in Angermünde, a period in which he developed leadership skills. His approach was based on *Auftragstaktik*, whereby a commander explains his objective to his subordinates and permits them to work out how this is to be done.

The Treaty of Versailles forced the closing of the General Staff, impelling the Reichswehr to send its officers out to train various men in a 4-year program of the hidden General Staff. In 1923 Manstein was called back to the General Staff where, though only a captain, he was tutoring those seeking to become part of the General Staff. In this demanding home study program, only a third of the original trainees successfully completed their studies.

On 1 February 1928, at age 40, Manstein was promoted to major, having served for thirteen years as a captain. When transferred to Dresden where he served from 1923 to 1927, Manstein taught military history and tactics, learning as he taught. From October 1927 to August 1929 he was Chief of Staff of a "shadow division" in Magdeburg.

He was next posted to the *Truppenamt* (Troop Office), an office of the disguised General Staff in Berlin, in October 1929. His task was to help prepare war games and staff rides, important parts of the education of a General Staff officer. On 1 April 1931 Manstein was promoted to *-Oberstleutnant* (lieutenant colonel). At this time the German Army engaged in the discussion of combined arms which, for example, resulted in the army and air force (*Luftwaffe*) working together in close air support for the invasion of France in 1940.

Manstein was also part of the secret German effort in the Soviet Union to develop tanks and aircraft, an activity in violation of the Treaty of Versailles. In 1931-32 Manstein traveled to the countries of some of Germany's potential future enemies, where he met leading generals and other officers. For example, he went to the Soviet Union in 1931 where he talked with military officers of the Soviet Army, such as Marshal Mikhail Tukhachevsky. Manstein was part of a group which in 1932 presented material on the origin of a parachute unit, and individually lectured on the dangers of friendly fire from artillery.<sup>2</sup>

In October 1932 Lieutenant Colonel Manstein assumed command of an infantry battalion in Kolberg, which gave him contact with soldiers again, a welcome change from staff work. When Adolf Hitler became Chancellor in January 1933, there were six million unemployed workers in Germany. Hitler began to partially solve this problem through government works, such as construction of the Autobahn. Although never a member of the Nazi Party, Erich Manstein was a supporter of Hitler until a couple of years into the war, when he saw Hitler's destruction of the German Army in the Soviet Union. Soon opposition to Hitler was crushed in 1933-34. Manstein was promoted to Colonel (*Oberst*) on 1 December 1933, which enabled him

## PROFILES IN INTELLIGENCE

---

to be appointed Chief of Staff of the *Wehrkreiskommando* III, a military area headquarters, in Berlin on 1 February 1934.

After he assumed authority in the *Wehrkreiskommando* III, Manstein wrote a well-known letter to Chief of the General Staff Ludwig Beck in which he opposed the ban on Jewish officers in the armed forces. This led to no changes in the treatment of Jews in the War Ministry and there is good evidence that Colonel General Beck and Colonel General Werner von Fritsch, Commander-in-Chief of the German Army, shielded Manstein as a promising officer. In the “Night of the Long Knives” on 30 June 1934, the Army supported the police action of decapitating the SA (*Sturmabteilung* or storm troopers), though Manstein condemned the killing of retired General Kurt von Schleicher, a former Chancellor.

When Field Marshal and President Paul von Hindenburg died, Hitler used the occasion to persuade all the officers and men of the German armed forces to swear an oath to himself on 1 August 1934, an oath which most felt they could not violate. This may explain why German generals failed to kill Hitler, when his decisions were destroying the Army in the Soviet Union (see below). General Ludwig Beck described this day as “the darkest day of my life.”

On 1 October 1936 Manstein was promoted to *Generalmajor* to become *Oberquartiermeister* (First Quartermaster General), or Vice Chief of the General Staff, where his main task was war planning. General Beck had changed the name of the *Truppenamt* to the Great General Staff. Manstein had a heavy load in his new position, but found relaxation by listening to music, gardening, and the study of history and architecture as an antidote to the long hours which he had to work. He made himself unpopular with some elements of the officer corps in Berlin by his outspoken ways. He had criticized Hitler for holding back the development of rocketry, though later Hitler began to be a supporter of the V (*Verwaltung* or Vengeance) rocket aimed on London. Manstein had sought to have a single service approach rather than three services competing with each other, an element of poison to many army officers in Germany and also in the United States and the United Kingdom today. Further, Manstein never suffered fools gladly, or people he considered to be fools.

### WORLD WAR II

Hitler’s expansionist plans were revealed to the Army leadership in 1937. Both Fritsch and General Werner von Blomberg, Minister of War, resisted Hitler’s plans and were sacked. Blomberg resigned on 27 January 1938 and Fritsch on 3 February 1938.<sup>3</sup> When officers were

summoned on 4 February 1938 to hear Hitler’s version of the Blomberg-Fritsch saga, Manstein shouted that it was a big lie. He was dismissed on the very next day, though he was kept in this position until he had led the incorporation of Austria into Germany (*Anschluss*). General Manstein planned Hitler’s invasion of Austria (March 11-12, 1938). Manstein next accompanied Col General Walther von Brauchitsch, Commander-in-Chief of the Army, to Vienna to investigate how the Austrian Army might be incorporated into the German Army. One of the results of this endeavor for Germany was to obtain some good officers, such as Colonel General Erhard Rauss, a panzer general. General Beck later sought to dissuade Hitler from any more foreign adventures but to no avail.

Manstein, having been dismissed as First Quartermaster, assumed command of the 18th Division on 31 March 1938, taking over from Lt General Hermann Hoth. Manstein continued in this position for 17 months, ending in the summer of 1938. On 1 April 1938 he was promoted to Lieutenant General. At this time Manstein approved of Hitler for having overcome Bolshevism and high unemployment, enabling Germany to avoid civil war.

Beck, in opposition to Hitler’s foreign policy, intended to resign. Manstein, aware of Beck’s plan, tried in vain to persuade Beck to change his mind. Manstein realized that Beck sought to restrain Hitler, who wanted to invade Czechoslovakia, but that Germany was not ready to fight its defenders, France and Great Britain. Beck resigned on 4 August 1938. Meeting British Prime Minister Neville Chamberlain in Munich in 1938, Hitler obtained the Sudetenland with its industry and border defenses of this region. During the Munich Conference, General Franz Halder, Beck’s successor as Chief of the General Staff, and General Hans Oster of Military Intelligence, both fearful that Hitler would start a world war, were planning a coup, which had to be called off when the Munich Agreement was signed on 29 September 1938. Consequently, Hitler came back to Berlin triumphant. Germany next created the protectorates of Bohemia and Moravia from the remains of Czechoslovakia.

### POLAND

Germany demanded the return of Danzig with road and rail links to East Prussia. Manstein was assigned as Chief of Staff to Army Group South under Col General Gerd von Rundstedt. Manstein heard Hitler demand that his officers and men “steel” themselves against humanitarian reasoning in the coming war with Poland. The Poles scattered their army along their frontier, having a reserve only along the Vistula near Warsaw. In comparison with the Luftwaffe, the Polish Air Force was outclassed in

terms of fighter planes, bombers, and number of well-trained pilots. The French, once counted on to save Poland from defeat, had a paper strength of over 100 divisions, whereas the British Expeditionary Force had only four divisions.<sup>4</sup> The Germans, having 3,600 armored vehicles, could advance from East Prussia, Slovakia, Pomerania, and Silesia. Further, they had 1,929 aircraft, whereas the Poles had only 900 planes.<sup>5</sup> The German strategy was to advance from different directions using mobile forces with powerful air support. In terms of weaknesses, they failed to develop operational or strategic depth and the Wehrmacht, having increased in size too fast, suffered from breakdowns in discipline. The German Luftwaffe did achieve surprise, and the German ground offensive developed into a rout. In flexible operations the various German commanders and troops were able to change their attacks from relatively strong to weak places in the Polish defense. On 25 September the Germans extended their air and artillery attacks on Warsaw, causing massive casualties—25,800 dead and approximately 50,000 wounded. Nevertheless, Manstein concluded in a letter to his wife: “I am very content and certainly proud (internally) about the success of our army group. One couldn’t hope for more.”<sup>6</sup> Manstein glossed over the fate of the Polish people in this and other instances, forgetting that the new Governor General of Poland was Hans Frank, a sadistic character. Great Britain and France failed to attack Germany’s western border, an area of minimal defense. In his later years Manstein said that he was surprised that the French and British did not invade Germany when German forces were occupied in Poland.<sup>7</sup>

### FRANCE AND GREAT BRITAIN

By 1940 the German Army numbered 102 divisions and 2.6 million men.<sup>8</sup> Manstein had supported General Heinz Guderian’s efforts to develop a *Blitzkrieg* strategy, the attempt to overwhelm an opponent using rapid movement, chiefly with tanks. Modernization of equipment, such as adoption of self-propelled artillery, continued at a rapid pace.

During the winter of 1939-40, the High Command sought to create a strategy for the invasion of France, but failed. It had recommended what was essentially the Schlieffen Plan from World War I, i.e., the invasion of Belgium into Northern France with the objective of defeating France quickly before concentrating forces on Russia.<sup>9</sup> That Plan had failed Germany. At that time Hitler had an intuitive grasp of the Schlieffen Plan and rejected it. Manstein was disliked by other German generals and so was sent back to lead an infantry corps in Stettin. Hitler replaced him with a man, General Franz Halder, who he could be fairly certain would do as he was told.

Hitler’s chief adjutant, Col Rudolf Schmundt, was a friend of Col Henning Tresckow, who influenced Schmundt to invite Manstein for breakfast with Hitler. General Manstein explained his strategic idea to Hitler. This involved one group of German armies invading Belgium and Holland as bait to persuade French and British generals to send their troops north. The main German attack would occur through the Ardennes, designed to race across France and place Allied troops in a vice. Rundstedt and Manstein fought a determined campaign for this strategy. Manstein’s principal concern was the possible threat of a French counterattack with tanks and planes from the south. This was met by attacks of the Luftwaffe. Other risks included inadequate logistical support. Hitler came to believe that this strategic concept was his, which would later persuade him in 1942 that he, not the German generals, should lead the attack on the Soviet Union, a fatal mistake.

Seven panzer and three motorized divisions were concentrated in Group A for the invasion of France through the Ardennes,<sup>10</sup> while Group B prepared to meet Allied forces by invading Belgium and Holland. The Germans could not be absolutely sure that their forces could get through the Ardennes, but were persuaded by intelligence studies that this could be accomplished. On 10 May 1940 the Germans attacked French and British forces. The problem of defending the southern flank of Group A was met through air power and Manstein’s infantry corps of 12 divisions which averaged 30 km a day despite the heat.<sup>11</sup> General Guderian and General Erwin Rommel raced across France to the Channel. This placed French and British troops between Group A and Group B in a cauldron of death. In six weeks the Germans had destroyed the armed forces of the Netherlands, Belgium, and France. Allied troops at Dunkirk escaped to England by boats of the British fleet and those belonging to private owners. The French government surrendered on 17 June and the British were driven off the continent. It was apparent that Manstein’s operational plans had succeeded beyond all expectations. *Generalleutnant* Erich Manstein, architect of one of the most decisive victories in military history, was promoted to *General der Infanterie* on 1 June 1940. This rank corresponds to that of a U.S. four star-general. For his exploits he also received the Knight’s Cross.

### RUSSIA

Germany’s intelligence on the Soviet Union was very limited. The KGB had maintained tight control around this nation, a counterintelligence feat that kept foreigners out with the result that German intelligence did not understand the industrial might behind the Urals. A geographic disadvantage for Germany



## PROFILES IN INTELLIGENCE

---

was that it did not have sufficient population from which to obtain an army large enough to cover the huge size of the Soviet Union. For example, when attempting to seize Stalingrad (see below), German military leaders were forced to depend on undependable Axis nations to guard their flanks, the result being disaster.

In terms of strategy, Manstein had no hand in planning the hoped-for invasion of England (SEALION) or the attack against the Soviet Union, despite his brilliant strategic concept for defeating France. Manstein later pointed out that Hitler and the High Command did not share a common strategic concept in the plan to move east, which was apparent in their approaches for this aggression. Hitler felt that the strategy adopted should have a dispersion of attack—center, north, and south—instead of a concentration of forces advocated by his military. Hitler stressed economic and political objectives, such as the conquest of the oil fields of the Caucasus, the factories of the Donets Basin, Leningrad, and Stalingrad, whereas Manstein in southern Soviet Union sought to destroy the enemy armed forces. As the Wehrmacht streamed into the Soviet Union, Hitler desired to conquer an area and then to maintain its control despite the costs, whereas Manstein utilized maneuver warfare which involved giving up land in order to destroy Soviet forces.

### CRIMEA

In the campaign against the Soviet Union, Manstein was initially in command of a mobile corps whose object was to conquer Leningrad. He tried as often as possible to go forward to see the action for himself. Because Manstein had demonstrated the ability to fight a determined opponent, on 12 December 1941 he was ordered to take command of the Eleventh Army in the southern part of the Soviet Union, a very happy development in his career. On 7 March 1942 he was promoted to *Generaloberst* (Colonel General). Hitler was desperate to gain the oil of the Caucasus, but this required conquest of the Crimea, an area from which the Soviets could attack the German flank or bomb the Romanian oil fields. The Eleventh Army was basically an infantry force in open country, lacking the necessary tanks, air power, and artillery. It included the XXX Corps, the XXXIX Mountain Corps, and the LIV Corps.<sup>12</sup> The Romanian Mountain Corps was added to Manstein's troops for the move toward Kerch to meet a Soviet landing. Manstein was aware of the weaknesses of the Romanian troops, one of which was the lack of a close relationship between officers and men.<sup>13</sup> He lacked artillery and thus called for air support, provided later by General Wolfram von Richthofen's VIII attack force. Soviet reinforcements, compounding Manstein's problems, began to pour into Sevastopol from 2 to 16 October.

Manstein was continually on the road visiting his troops, and in the process exposing himself to danger. He had to contend with the poor roads of Crimea, the continuous rains in November which changed these roads into mud, and the control of the Black Sea by the Red Navy, making his task even more difficult. Manstein's army was at the end of a long supply line. At this time Manstein did send out an unfortunate message that the Jewish-Bolshevik system must be wiped out. Nevertheless, in the postwar trials he was found guilty of the murder of Jews, gypsies, partisans, and communists.

The Soviet landings on the Kerch Peninsula at Feodosia in late December 1941 were a danger to the Eleventh Army and to its efforts to take Sevastopol. The Soviets eventually had 17 rifle divisions, three rifle brigades, two cavalry divisions, and four armored brigades on the Kerch Peninsula.<sup>14</sup> Manstein had only seven German infantry divisions, plus a regiment, under his command before the arrival of reinforcements. With the Soviet landing Manstein was thus fully committed on two fronts. He decided to destroy the enemy force on Kerch before assaulting Sevastopol. Manstein's skill saved the situation, as he improvised, used his intuition, and utilized the Romanian Mountain Corps and Tatars. Richthofen's VIII Air Force, arriving on 21 April 1942, was used in the effort to wipe out the Soviet hold on the Kerch Peninsula. In his summary of the Kerch victory, Manstein gave credit to air power led by Colonel General Wolfram von Richthofen. However, VIII Air Corps' support could only be temporary, because it was needed to reinforce Army A in its drive against the Soviet Union.

For the second major attack on Sevastopol, Manstein massed 611 guns, 754 mortar tubes and rocket launchers, two 60-mm mortars, and an 80-cm giant cannon, along with employing air attacks between 2 and 7 June 1942 to break the stronghold's defense.<sup>15</sup> In a week of fighting the average German rifle company strength was down to 20-30 men.<sup>16</sup> On 27 June Manstein launched the final attack on Sevastopol. When the city fell on approximately 4 July, 90,000 Soviet military personnel were captured. For his achievement Manstein was promoted to Field Marshal on 1 July 1942.

### STALINGRAD

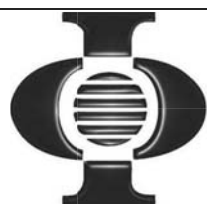
In September 1942 Hitler sacked Field Marshal Wilhelm List, commander of Army Group A, during his drive on Stalingrad, and replaced him with Manstein, who on 22 November 1942 was appointed to command the newly created Army Group Don. Hitler had divided his forces by sending Army Group A into the Caucasus to seize the Baku oil fields in order to supply the German war machine with this precious commodity. Hitler also assigned Army

## PROFILES IN INTELLIGENCE

Group B to capture Stalingrad, essentially an object of prestige. This was a difficult period in Manstein's life, since his son, Gero, had been killed in action on 29 October 1942, resulting in a period of mourning.

Stalin had approved of Operation URANUS, designed to destroy German forces at Stalingrad, and Operation SATURN, the goal of which was to destroy Axis armies in the southern part of the Soviet Union. German military intelligence did not observe Stalin's buildup around Stalingrad where Army Group B's Sixth Army was in an exposed position, because its flanks were guarded by comparatively weak Rumanian, Italian, and Hungarian units. The Soviets surrounded Stalingrad on 23 November 1942. Manstein, sent to rescue the Sixth Army, did not assume command of Army Group B until six days later. Should the German Sixth Army, commanded by General Friedrich Paulus, have ordered a breakout immediately? Instead of sending representatives to Paulus, should Manstein have visited the pocket to assess the situation, even though weather conditions probably made it inadvisable for him to make this venture? Manstein doubted the ability of the Sixth Army to break out without the aid he did not have. With the exception of Manstein, sometimes blamed for the loss of the Sixth Army, German army and air force generals felt that Paulus should break out of the trap immediately.

The Luftwaffe was not able to provide the Sixth Army with the necessary supplies of food, ammunition, and medicine, making ridiculous Goering's promise that he could provide 600 tons of these supplies daily. He had not even consulted his staff which was unanimous in the belief that this offer was not possible. During the ordeal of the Sixth Army, Goering left to go to Paris on an art-hunting expedition. Field Marshal Manstein also had to be concerned about the planned Soviet attack on Rostov-on-Don, which if successful would have trapped both Armies A and B for eventual extermination or surrender. On 26 November Hitler rejected Manstein's recommendation to pull back the Sixth Army and withdraw perhaps as far as the Dnieper River. Manstein was very much concerned that the Soviets would trap Army Group A in the Caucasus. On 28 November General Kurt Zeitzler, Chief of the *Oberkommando des Heeres* (OKH), informed Manstein that the Fuehrer had ordered that Stalingrad must be held at all costs, a decision based on the desire to recoup prestige rather than on strategic requirements. Manstein did not have the necessary forces to hold Stalingrad, nor did he receive significant reinforcements. The relief attack for Stalingrad finally occurred on 12 December 1942, when the two German divisions of Austrian Major General Erhard Rauss were repulsed by the Soviets. The Sixth Army was unable to meet Rauss' force due to shortages of fuel and ammunition. On 17 December another attempt, this one under General Frido



# PLURIBUS INTERNATIONAL

*Excellence with Integrity*

**Pluribus International Corporation provides high quality, best-value, intelligence analysis and programmatic support services to U.S. Defense, Homeland Security, and Intelligence Community customers that directly support the fulfillment of National Security objectives. Honesty and integrity in our actions and dealings with customers, employees, and industry partners will never be compromised.**

**For information contact Todd Spires, Director of Business Development  
todd.spires@pluribusintl.com (571) 297-4432**

**[www.pluribusinternational.com](http://www.pluribusinternational.com)**

von Senger und Etterlin, failed to relieve the Sixth Army. On 18 December Manstein requested permission from Hitler to order the Sixth Army to break out, but this and one more request were denied.

When Stalingrad fell, Army Group A was still in the Caucasus. The German Army had suffered 100,000 casualties and 90,000 POWs at Stalingrad with only 5,000 German troops returning from the horrifying Soviet POW camps. The battle for Stalingrad had, however, tied down seven Soviet armies,<sup>17</sup> helping other German divisions escape their planned encirclement by the Soviets in URANUS.<sup>18</sup> Manstein was very much aware of this contribution by the Sixth Army.<sup>19</sup>

### COUNTERATTACK

In response to Manstein's and Zeitler's urging, on 29 December Hitler finally permitted Army Group A to evacuate the Caucasus before the Soviets could trap it. In early 1943 Manstein had disputes with Hitler, disputes which continued until his dismissal in 1944. Hitler, convinced of the utility of a static defense from World War I, opposed loss of the Donets or any territory. Field Marshal Manstein conducted mobile operations, which involved loss of territory in the effort to trap enemy troops. The Soviets began a series of constant operations, keeping German officers off balance. Manstein feared that most of or the entire German southern wing would be trapped by these moves. He turned his attention from Stalingrad to the salvation of the southern wing of the German Army.<sup>20</sup> His defensive strategy was to surrender territory and entice the Soviets to overextend themselves, and when their offensive culminated, he would counterattack. In accordance with the German way of war, he planned to withdraw from the Lower Don and Donets, and concentrate around Kharkov from which he could counterattack. Hitler's decisions, seen by Manstein as interference, often came too late to meet an unfolding operation. Hitler bitterly opposed Manstein's methods and they argued with one another on a daily basis. Manstein urged the Fuehrer to establish his own military advisor, but Hitler, who repeatedly described himself as the greatest warlord of all time, rejected this suggestion.

The Soviet offensives, Operations GALLOP and STAR, threatened to overwhelm Germany's entire southern wing. Beginning on 20 February 1943, Manstein launched his counteroffensive by striking the flanks and rear of overextended Soviet forces with panzer divisions.<sup>21</sup> Soviet troops fled the attack which killed approximately 23,000 Soviets troops.<sup>22</sup> In addition, Panzer forces destroyed or captured 156 tanks and 178 guns.<sup>23</sup> Manstein had one division to his opponent's eight, demonstrating brilliance on his part. On 14 March 1943 Manstein recovered

Kharkov, again defeating the Soviets, his object being the defeat of Soviet troops rather than seizing land.<sup>24</sup> This was in accordance with the strategy of General Carl von Clausewitz rather than that of Corporal Hitler.<sup>25</sup>

### KURSK

The Battle of Kursk in July 1943 is regarded by some historians as the turning point of World War II. However, German military historian Karl-Heinz Frieser disagrees with this analysis, calling the battle only "an embarrassment." He states that the battle had no strategic goal, only a defensive one, since Hitler and the High Command sought only to establish a defensive line and to weaken the Red Army sufficiently to avoid a massive summer attack.<sup>26</sup> The German High Command wanted to use this battle, which they called Citadel, to shorten its front and wear down Soviet reserves. Hitler insisted on delays in mounting the German offensive which gave the enemy time to make massive defensive preparations. Manstein was frustrated by the lack of urgency in this operation. On 20 March he demanded an immediate counteroffensive, a request that Hitler refused. On 30 March 1943 Manstein returned to Germany to attend to problems with his eyesight. As Hitler postponed the date of the German attack, the Soviets continued to build up their defenses. Manstein argued with Hitler, seeking an end to these delays. Hitler justified these obstructions on the basis that soon heavy armor—Tiger tanks and Ferdinand tank destroyers—would be available for this battle. This argument does not make sense, because new weapons usually demonstrate considerable weaknesses until these problems are worked out. Hitler postponed the attack until 5 July. Manstein was to attack from the south of the salient and Field Marshal Walther Model from the north.

Karl-Heinz Frieser, with access to Soviet archives, could assess Soviet preparations with reasonable accuracy. According to his statistics, for this battle the Soviets had 1,987,463 troops, whereas the Germans possessed only 625,271; Soviet tanks were 8,200 to 2,699 for the Germans; Soviet artillery consisted of 47,416 while the Germans had 2,699; the Soviets possessed 5,965 planes and the Germans 1,372.<sup>27</sup> The Germans inflicted 3:1 casualties against the Soviets, but could not survive the loss of equipment during this battle. The Soviets lost 400 aircraft in one day and 200 the next day,<sup>28</sup> but their overwhelming superiority in numbers prevented this loss from being significant. Manstein and Model from the north could not destroy the massive Soviet defenses which had accumulated while Hitler dithered. German intelligence had scant knowledge of the strategic depth of Soviet defenses as listed above. Major General Mungo Melvin sees this battle as a defeat for Manstein, but how could any commander overcome Hitler's constant subversion of the German Army? Army Group

Center ordered Model to turn around and face a new threat, a Soviet move near Orel, an area behind him. On July 13 Hitler called both Field Marshals Manstein and Kluge to his East Prussian headquarters and informed them that he had called off Citadel because of the expected attack on Sicily, which did occur on July 9-10.<sup>29</sup> Manstein insisted that the attack continue, but Hitler was Germany's dictator.

### FIGHTING ON TWO FRONTS

After Citadel was called off, the initiative on the Eastern Front passed to the Soviets due to their massive defenses, something the Germans failed to crack. Manstein could only slow down the Soviet attack. Manstein bore the brunt of the Soviet attack that lasted from Citadel until September 1944 when the Soviets forced Romania to capitulate. His defensive strategy was to concentrate from a less threatened sector to a more endangered one in this vast area to be defended. German weakness allowed the Russians to penetrate the overextended land from when and where they wished.<sup>30</sup> His army had insufficient logistical and artillery support. Infantry units fought continuously and were worn out, resulting in their increasingly weakened performance. "For a casualty total of 133,000 men, he had received only 33,000 replacements..."<sup>31</sup> Requests for retreat were usually denied, and promises of reinforcements were not met. Hitler's decisions at this time can be defended. He had to have reserves to counter Allied landings in Italy and possible threats of attacks on the Balkans and France and so could not meet Manstein's urgent needs.

The German generals grew increasingly restive as the Soviets pushed back toward the German border. However, Manstein believed that a Prussian field marshal must not mutiny against the political leadership. On 3 September 1943 Manstein and Field Marshal Hans-Guenther Kluge met and confronted Hitler where they demanded that he appoint a military commander in the East to coordinate the four army groups on the Eastern Front. As usual, Hitler refused to yield authority to a military officer. However, acting on his own, Manstein ordered a retreat to the Dnieper River on 15 September 1943, for which he did not have enough troops to cover this operation. In this movement Manstein used the scorched earth method, which led to the accusation of a crime when he was later tried at Nuremberg.

Lt General Henning von Tresckow visited Manstein on 25 November 1943, arguing that Germany under Hitler would be defeated and calling for his removal. Manstein was firm in his refusal to participate in a coup. When Hitler dismissed Manstein in March 1944, the Field Marshal expressed the hope of another command that never materialized. After the German surrender he became a prisoner of the British Army in May 1945.

### IMPRISONMENT

At the Nuremberg trials Manstein defended the Wehrmacht's conduct and the honor of the German General Staff by attributing the numerous war crimes to Hitler. Manstein helped Dr. Hans Laternser, the main defense counsel, prepare the case for the German Army and generals. His main theme was that commanders and soldiers should not be branded as criminals for defending their country. Manstein said he knew nothing about the existence of concentration camps or the activities of the *Einsatzgruppe*, which sought out and murdered Jews in the Soviet Union. After his questioning, Manstein was transferred to the custody of the British where he was placed in Wales on an island farm on 2 September 1946. He lived in a block house with Field Marshal von Rundstedt and Col General Walther von Brauchitsch. Having given their word of honor, these senior officers were permitted to go into town unescorted.

On 22 July 1948 Manstein and Rundstedt were sent to London and from there to Nuremberg, the decision to prosecute having been made by the British Labor government. Many British officers opposed such trials, based on the need to gain German support in the event of a Soviet attack. Winston Churchill attacked the Labor government for wrongful procedure against German generals. On 19 December 1948 Manstein was found guilty of doing nothing to prevent the slaughter of Jews in the Crimea and sentenced to eighteen years in prison. He was sent to a prison in Werl near Dortmund.

While imprisoned, Manstein did not admit to any guilt, his own or that of his troops. From May 1950 he concentrated on writing *Verlorene Siege (Lost Victories)*, a highly successful book which appeared in German in 1955 and in English in 1958. The reviews in both languages were excellent. When Churchill was reelected as prime minister in 1951, the atmosphere had improved. Many German ex-soldiers, on whom rearmament depended, made it clear that they would not serve as long as the British imprisoned Manstein and Field Marshal Albert Kesselring, previously commander of German defenses in Italy. Having been home since 1952 to be with his severely ill wife and having his own operation, Manstein was released from house arrest on 7 May 1953 after eight years of imprisonment and detention. Germany entered NATO in 1953 and founded the *Bundeswehr* in 1955. When the *Bundeswehr* was being formed, Manstein recommended that new divisions be composed of three strong brigades, which NATO armies eventually adopted in "similar" forms.<sup>32</sup>

In 1966 Manstein's wife of 46 years died. Manstein's last years were spent in reading and meeting regularly with former colleagues General Walther Wenck, General Theodor



## PROFILES IN INTELLIGENCE

---

Busse, and General of the Cavalry Siegfried Westphal. When Manstein celebrated his 80th birthday, an army choir entertained him and his guests. On 15 June 1973 he died at age 86 and was buried with full military honors.

### DESIRABLE TRAITS IN AN INTELLIGENCE LEADER AS DEMONSTRATED BY MANSTEIN

Field Marshal von Manstein was able to develop a strategy to take advantage of French weakness and successfully urge the German government to utilize it for the defeat of France. The East German intelligence leader, Markus Wolf, identified the main weakness of the West German government—namely, millions of its young men were killed in the Second World War with the result that many young women did not find husbands. When they eventually reached positions of secretary or administrative aide to men in high positions in the West German government, Wolf sent his “romeos,” or men who would seduce and/or marry these women in order to gain access to critical information in the West German government.<sup>33</sup> Both Manstein and Wolf could spot a weakness in the enemy and take advantage of the situation. This is a desirable trait for an intelligence leader.

Manstein set a trap for his enemy in the Soviet Union immediately after the German defeat at Stalingrad. The term “trap” is meant as a situation in which a leader persuades or allows the enemy to move into a certain area before attacking. Manstein waited until Soviet lines were overextended in 1943 and then attacked them with Panzer forces, killing approximately 23,000 Soviet troops. In World War II in the Pacific, U.S. Navy cryptanalysts had broken the main Japanese naval code (JN-25) sufficiently well by June 1942 that they knew that a Japanese naval contingent was en route to the Midway atoll. Remaining silent, the U.S. Navy ambushed the Japanese in June 1942 and, destroying four carriers, assured American naval dominance in the Pacific for the remainder of the war. Intelligence leaders should have the ability to set traps for opponents.

Manstein was able to construct a profile of Adolf Hitler, his political leader. He found out that Hitler would not tolerate the appointment of a commander of forces in the East, despite his acceptance of responsibility for the Stalingrad debacle; that he resisted maneuverability, insisting that every foot of captured territory should be maintained in a static defense; that he had no real training in strategy and grand tactics;<sup>34</sup> that he overestimated the importance of the will; and that he could not be taught. An intelligence leader may have a personality profile of his political leader created by his subordinates, but in the last analysis he must depend on his own diagnosis of his superior. If he is wrong, it will be very difficult to manipulate the political leader.

Manstein had experience at various levels in the army—he was staff officer in a regiment, battalion, and at the General Staff level and commanding officer of a company, a battalion, a division, a corps, and an army group. As such, he had learned various levels of the German Army and how to utilize them in warfare. An intelligence leader should have experience at as many levels of the intelligence community as possible. The exception is the stellar performance of John McCone, a complete outsider to intelligence, as Director of Central Intelligence.

Field Marshal von Manstein was persistent in his pursuit of goals—such as the conquest of Sevastopol. William Colby, former Director of Central Intelligence, was determined to defend the CIA from Congressional attack to the extent that he gave his questioners the “Crown Jewels,” a summary of alleged misdeeds of the Agency. This represented his effort to prevent Congressional staffers from inflicting a “thousand cuts,” an extended period of public revelations. Colby believed this could endanger the existence of the CIA. As Colby pursued this goal, he suffered a litany of complaints and verbal attacks from his friends and members, both active and retired, of the intelligence community.

### HONOR

Manstein demonstrated honor in that during his trials he defended the conduct of the German Army and German officers in World War II, despite the fact that he knew full well this might adversely affect the decision of his judges. An intelligence leader must have the honor to defend his agency against assaults from leftist members of Congress, even if he knows his action will lead to his dismissal.

Field Marshal von Manstein could withstand uncertainty, the possibility of defeat, and the encirclement of his armies after the defeat of Stalingrad in early 1943. Intelligence leaders must be able to withstand constant uncertainty, since intelligence by its very nature is characterized by gnawing suspicion and perhaps adverse investigations.

Manstein’s traits and abilities, as outlined above, are important for an intelligence leader to possess. Selection committees for the choice of these men and women would do well to keep Manstein’s competencies in mind as they sift through candidates for these positions.

### NOTES

<sup>1</sup> Major General Mungo Melvin, *Manstein* (New York: St. Martin’s Press, 2010), p. 27. I am dependent on this source for accurate dates. This excellent volume is the first important work in English and is highly recommended.

<sup>2</sup> Manfred Zeidler, *Reichswehr und Rote Armee 1920-1933* (New York: St. Martin's Press, 2010), pp. 215, 252.

<sup>3</sup> Field Marshal Blomberg was forced to resign once it was learned that he had married a former prostitute and Colonel General von Fritsch was forced to resign on a false charge of homosexuality.

<sup>4</sup> Melvin, op. cit., p. 119.

<sup>5</sup> Ibid., p. 120.

<sup>6</sup> Ibid., p. 125.

<sup>7</sup> Ruediger von Manstein, *Soldat im 20. Jahrhundert* (Vienna, Austria: 2002), p. 86.

<sup>8</sup> Melvin, op. cit., p. 79.

<sup>9</sup> Christoph Cornelissen, "Schlieffen-Plan," *Enzyklopaedie Erster Weltkrieg* (Munich, Germany: Ferdinand Schoening, 2003), pp. 819-820.

<sup>10</sup> Melvin, op. cit., p. 158.

<sup>11</sup> Ibid., p. 179.

<sup>12</sup> Ibid., p. 230.

<sup>13</sup> Erich von Manstein, *Lost Victories* (Novato, CA: Presidio Press, 1958), p. 207.

<sup>14</sup> Melvin, op. cit., p. 158

<sup>15</sup> Ibid., p. 263.

<sup>16</sup> Ibid., p. 267.

<sup>17</sup> Ibid., p. 312.

<sup>18</sup> Dana V. Sadarananda, *Beyond Stalingrad* (Westport, CT: Praeger, 1990), p. 44.

<sup>19</sup> Erich von Manstein, op. cit., p. 441.

<sup>20</sup> Ruediger von Manstein, op. cit., p. 162.

<sup>21</sup> Sadarananda, op. cit., p. 117.

<sup>22</sup> Melvin, op. cit., p. 342.

<sup>23</sup> Ibid., p.341.

<sup>24</sup> Erich von Manstein, op. cit., 433.

<sup>25</sup> Carl von Clausewitz, *On War* (edited and translated by Michael Howard and Peter Paret) (Princeton, NJ: Princeton University Press, 1976), p. 181.

<sup>26</sup> Karl-Heinz Frieser, "Die Schlacht im Kursker Bogen," *Das Deutsche Reich und der Zweite Weltkrieg* (Munich, Germany: Deutsche Verlags-Anstalt, 2007), p. 170.

<sup>27</sup> Karl-Heinz Frieser, op. cit., p. 101.

<sup>28</sup> Melvin, op. cit., p. 372.

<sup>29</sup> Ruediger von Manstein, op. cit., p. 174.

<sup>30</sup> Sadarananda, op. cit., p. 99.

<sup>31</sup> Melvin, op. cit., p. 387.

<sup>32</sup> Melvin, op. cit., p. 500.

<sup>33</sup> Kenneth J. Campbell, "Marcus Wolf: One of History's Most Effective Intelligence Chiefs," *American Intelligence Journal*, Vol. 29, No. 1, 2011, pp. 148-157.

<sup>34</sup> Erich von Manstein, op. cit., p. 275.

*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. Ken can be reached at [drcampbell@comcast.net](mailto:drcampbell@comcast.net). He is a frequent contributor to this Journal and in particular to its historical "Profiles in Intelligence" series.*




**PARSONS**

**Design.  
Deploy.  
Defend.**

**Engineering a Safer World.**

[www.parsons.com](http://www.parsons.com)

proven value  SM

## NMIA Bookshelf

### ***DISCIPLES: THE WORLD WAR II MISSIONS OF THE CIA DIRECTORS WHO FOUGHT FOR WILD BILL DONOVAN.***

Douglas Waller.

New York, Simon & Schuster Press. 2015.

454 pages.

**Reviewed by Col (USAF, Ret) John R. Clark, a member of the NMIA Board of Directors, an emeritus member of both the NMIF Board and the DIAA Board, and a former adjunct professor at the Joint Forces Staff College.**

Best-selling author Douglas Waller was searching for a follow-on project after publishing his highly respected book *Wild Bill Donovan: The Spymaster Who Created the OSS and Modern American Espionage* (reviewed in *AIJ*, Vol. 29, No. 2, 2011). The National Archives expert on the OSS suggested Waller consider the four OSS officers who fought in World War II and ultimately became Director of Central Intelligence (DCI). General Donovan, head of the OSS in World War II, was the leader, mentor, and inspiration for Allen Dulles, Richard Helms, William Colby, and William Casey—all of whom became head of the CIA.

Each man had a unique background, skillset, and role—first in the OSS during the war, and later in the CIA in various positions. To understand the story behind the story, Waller divides the book into three parts: Preparation, World War II, and the Cold War. In the Preparation section, Waller provides the family history, education, and skillsets of the individuals' work and military history prior to the war. In the World War II section, he dutifully tracks the four principals into their OSS wartime roles, their relationships with Allied counterparts (especially the British Special Operations Executive), covert missions with military special forces, and the authorities for these missions. This section contains information on a wide variety of programs run by the OSS, and many fascinating anecdotes on the outcome of these programs. Next is the Cold War section in which Waller explains the post-World War II wrap-up and dissolution of the OSS. Finally, Waller provides a concise summary of the four as DCIs during the Cold War covering their challenges, complex relationships, and a candid look of the outcome of their leadership as DCI.

In taking on this project, Waller intensively researched manuscript documents, family collections, reminiscences, interviews, and government reports including materials in the National Archives. His book provides a unique look

from the inside at the how and why the OSS was formed and organized, and the roles that Donovan's lieutenants had in establishing it. He pulls no punches, and applies no filter—an excellent tutorial on American intelligence history. Many of the lessons learned are currently core to current intelligence collection and covert operations. One complaint is that the section on the Directors could be more detailed—but that may be his next book. In addition, because all four served in the European Theater, the orientation is on Europe and does not include the Far East.

To thread the four "Disciples" together, Waller starts with Dulles, who was the first of the four to be selected as DCI, and ran CIA very similarly to the way Donovan ran the OSS. He viewed the CIA's mission as providing intelligence collection to avoid another Pearl Harbor, and to launch covert operations to alter the course of events overseas. This emphasis on covert action leads to the failed invasion of Cuba by exiles at the Bahia de Cochinos, also known as the Bay of Pigs. Ultimately, President Kennedy loses trust in Dulles, and the DCI is forced to resign.

Helms, the consummate spy, as DCI focused on intelligence-oriented thinking and planning. As Congress exercised its oversight role, Helms testified to various committees on the past activities of CIA. Unfortunately, he did not divulge information deemed too sensitive to release to Congress. When President Nixon fired Helms in November 1972, it was reportedly due to a failure to reorganize the "bloated and ineffective" national Intelligence Community. However, Helms believed he was relieved due to permitting his deputy, LTG (USA) Vernon Walters, to refuse to allow the administration to involve CIA in the Watergate debacle.

Colby headed the Civil Operations and Revolution and Development Support (CORDS) element in Vietnam, and was then selected to head the Far East Division at CIA Headquarters. Colby was the next of the four to be picked as the head of CIA. His tenure was marked by the controversial release of the Agency's "Family Jewels," and the resultant fallout. One of the reactions to the disclosure of these sensitive programs was the Congressional accusation that Helms committed perjury during his previous testimony. Consequently, he negotiated a plea deal to avoid a felony conviction. This created a rift between Helms and Colby that was never resolved, and it also permeated CIA.

Waller provides intimate information and anecdotes throughout the book on the four Disciples and their personal and professional lives. His research and organization of the



book are outstanding. His bibliography, source notes, and acknowledgments are impressive. If one reads nothing else, it is wise to follow Bill Casey's guidance on reading nonfiction—start at the back (the bibliography, source notes, and acknowledgments), focus on the key areas, and skim the rest. It also must be considered that in the Intelligence Community the missteps and warts are fully exposed, but knowledge of the successes and victories are often diluted by clearance restrictions and sensitivity considerations. The CIA is no different, and even more vulnerable to oversight efforts from Congress. Waller presents a comprehensive, introspective view of the OSS and the CIA, and the four DCIs that helped create the modern CIA. It is a great read on a very important element of American intelligence, and its impact on the current national Intelligence Community.

• • • • •

### ***PLAYING TO THE EDGE: AMERICAN INTELLIGENCE IN THE AGE OF TERROR***

Micheal Vincent Hayden.  
New York, Penguin Press. 2016.  
448 pages.

**Reviewed by Dr. Edward M. Roche, of the Columbia Institute for Tele-Information, under the business school of Columbia University, from which he holds a PhD, and the Grenoble Ecole de Management. He is also a lawyer and the author of "The Cyber Intelligence of Asynoptic Networks" and the "Industrial Espionage" section of *The Guide to the Study of Intelligence*, published by the Association of Former Intelligence Officers (AFIO).**

*Playing to the Edge* is authored by a 1980 graduate of the National Intelligence University (NIU), Gen (USAF, Ret) Michael V. Hayden, the only person ever to serve as head of both the National Security Agency (NSA) and the Central Intelligence Agency (CIA). He accomplished this during very tumultuous times, including the controversy over enhanced interrogation and the security breach by traitor Edward Snowden, which Hayden describes as "the greatest hemorrhaging of legitimate American secrets in the history of the republic" (p. 421). The author has had a life-long career in intelligence. In the 1980s he served as the Air Attaché to Bulgaria, where he recalled that after having his car tailed for several hours by the Bulgarian security services they pulled up alongside and motioned that it was time to get lunch (p. 314).

Much of the book discusses Congress, the press, and the handling of numerous public controversies regarding intelligence. These experiences gave Hayden a sober view of the press. "Be careful what you tell these people. Some

are less interested in honest dialogue than listening to rebut and accuse and discredit" (p. 400). He writes about a hypothetical discussion with an intelligence case officer: "It's authorized by the president [and the] attorney general [and] Congress" have been briefed. But "have you run it by the ACLU? What does the *New York Times* editorial board think?" (p. 382) However, the author also used the press. He lauds the website <http://ciasaveslives.com> (p. 397) and with Mike Mukasey (81<sup>st</sup> Attorney General of the United States (2007-2009) published a powerful editorial in *The Wall Street Journal*.<sup>1</sup>

On Congress the author notes, "One congressman wanted to know whether or not CIA complied with "Buy America" legal requirements for construction materials used in black sites overseas" (p. 229). Advice for briefing Senator Wyden: "Speak slowly" (p. 183). Hayden often expresses frustration: "There are days when a director of CIA is inclined to think that he is running a large public affairs, legal, and legislative liaison enterprise attached to small operational and analytic elements" (p. 232).

Hayden covers NSA controversies surrounding the Prism and Stellarwind programs, and his book is full of details regarding how public policy was discussed and decided. The same is true on the CIA side, where enhanced interrogation and targeted killings stormed into the public debate. He has clear and compelling views on these matters. On enhanced interrogation: "[T]he facts of the case are that the use of these techniques against these terrorists made us safer. It really did work" (p. 386). "[T]he targeted killing program has been the most precise application of firepower in the history of armed conflict" (p. 341). Moreover, "The United States will need to keep this capacity and be willing to use it" (p. 344). Hayden expresses irony concerning the prohibition of CIA detentions: "We had finally succeeded in making it so legally difficult and so politically dangerous to grab and hold someone that we would simply default to the kill switch to take terrorists off the battlefield" (p. 242).

The book does not go into detail regarding operations. Hayden does not "talk." He devotes an entire chapter on intelligence thinking surrounding the bombing of the North Korean-built nuclear reactor near Al-Kibir, Syria, but never mentions who did it. This fits in with his general view of the value of secrecy. "Espionage thrives in the shadows, and secrecy is an essential component of its success. Despite a latent plus side (legitimacy, support, understanding), American intelligence has traditionally judged the minus side of going public (decreased effectiveness) to be determinative" (p. 422). He repeats the advice Richard Helms gave to Robert Gates: "Never go home at night without asking yourself, 'Where is the mole?'" (p. 278).



*Playing to the Edge* is full of interesting anecdotes and descriptions of notable persons. President George W. Bush liked to call Hayden “Mikey” as in “Mikey, get in here!” (p. 372) On Attorney General Eric Holder: “Messianic in his focus, politically tone-deaf, and indifferent to contrary evidence and views” (p. 395). On Senator John McCain: “The election of John McCain would have been more disruptive to the way America produced intelligence than the election of Barack Obama” (p. 354). Hayden describes Rahm Emanuel, Obama’s former Chief of Staff, as congratulating CIA on the targeted killing of an al-Qaeda member (p. 342). On Abdullah II of Jordan: “When the king is in the United States, he motorcycles our back roads in the company of a close American friend, a former CIA senior” (p. 322). On Saudi Arabia’s King Abdullah’s views of Iran: “Cut off the head of the snake” (p. 320). On Obama and Netanyahu: “I suspected that the two men talked past each other” (p. 299). Director Leon Panetta trying to encourage CIA employees potentially threatened by release of information regarding enhanced interrogation was like a “pep rally in the Führer bunker” (p. 382). On former CIA directors: “It would be hard to get them all to agree that a certain day was Tuesday” (p. 393). On angling to start briefing candidate Obama: “We would work to get access to him and then create as many of what we crudely called ‘aw, shit’ moments as possible” (p. 356). On the Iranians: “They *will* cheat, of course. It’s what they do” (p. 309). On the head of the Afghan National Directorate of Security while visiting Colonial Williamsburg: “Where are the walls?” “Walls?” “Yes. To protect them from the people” (p. 316).

Regarding NSA, Hayden mentions “the director’s massive conference table, which looks like it was ripped off the set of *Dr. Strangelove*” (p. 172). He describes a secret visit to Pakistan with VADM (USN, Ret) Mike McConnell. Upon departure, their jet needed to refuel. “The crew had forgotten their government credit card—you can’t make this stuff up—and the Pakistanis wouldn’t budge” (p. 348). Consequently, the DNI and the CIA Director were sitting on the tarmac in Pakistan with empty fuel tanks.

The author describes National Intelligence Estimates (NIEs) as having “arcane style [and] language” (p. 297). However, he himself has a quirky habit of adding the word “period” to the end of sentences, as in: “This does not authorize the collection of content, period” (p. 408), referring to one program; “[O]ff the table. Period.” (p. 381); and “[W]aterboarding . . . hadn’t been used for almost five years. Period” (p. 242).

*Playing to the Edge* is a valuable insider’s account of how the Intelligence Community navigated through difficult years during the Bush and Obama

administrations. It is primarily about the practical handling of public controversy and the nature of the public debate regarding the role of intelligence in American society. Hence, it is perfect reading for anyone interested in public policy. In addition, it provides a bird’s-eye view of challenges faced by managers in intelligence, and some of the practical ways to handle reform.

General Hayden ultimately is an optimist, and he believes in people. In spite of all the challenges to the Intelligence Community, he insists that “good people overcome imperfect structures” (p. 178). Nevertheless, do not look to him for any leaks about intelligence. That is not what he does.

## NOTE

<sup>1</sup> Michael Hayden and Michael B. Mukasey, “The President Ties His Own Hands on Terror: The Point of Interrogation Is Intelligence, Not Confession,” *The Wall Street Journal*, April 17, 2009, <http://www.wsj.com/articles/SB123993446103128041>.

• • • • •

## ***THE FIELD OF FIGHT: HOW WE CAN WIN THE GLOBAL WAR AGAINST RADICAL ISLAM AND ITS ALLIES***

LTG (USA, Ret) Michael T. Flynn and Michael Ledeen.  
New York, St. Martin’s Press. 2016.  
194 pages.

**Reviewed by George W. Ridge, former Dean of the University of Arizona Journalism School, a reporter and editor for such newspapers as *Stars and Stripes* and *International Herald Tribune*, and who for 15 years wrote approximately 850 published travel columns. In addition, he and his wife wrote a weekly review of Tucson restaurants for the *Arizona Daily Star*. He has previously reviewed books for such scholarly journals as *Military Review*.**

Michael Flynn rose to the top of the U.S. Defense Intelligence Agency only to, in his own words, be “summarily fired.” He says his dismissal came because he told a Congressional committee that the U.S. was not as safe as it had been a few years back (other sources report that the firing was due to bad management). Now retired, and fairly quickly reemerging as the principal advisor on military affairs to Republican Presidential candidate Donald Trump, Flynn thrust the dominant question of the 21st century into the middle of the 2016 Presidential campaign: How can the United States bring together a cohesive strategy to lead the global fight against radical Islam?

“We’re still in a world war, but very few Americans recognize it, and fewer still have any idea how to win it,” the authors conclude.

Among Flynn’s disclosures, he tells about high-level censorship of intelligence reports, possibly from the Oval Office down. He pointed out that “in the summer of 2015, dozens of military analysts protested that their superiors at the central command for the war in the Middle East (CENTCOM) were blocking or altering their reports.” [Editor’s Note: See my amplifying comments on this controversial topic in the “Editor’s Desk” section at the beginning of this volume.]

Flynn relies on his teamwork with GEN (USA, Ret) Stanley McChrystal in Iraq and Afghanistan to formulate the beginnings of his own strategy, spicing the narrative with vignettes to which only those from the battlefield could relate. He remembers vividly the welcome-to-Afghanistan fireworks that the Taliban dropped off at McChrystal’s headquarters—a vehicle bomb. “Things had to change and change fast—we were losing.”

Among the numerous reforms effected was abandonment of the centuries-old interrogation of prisoners through the use of paper maps. “We literally taught detainees how to use a Google map with a mouse and laptop.” It was fun for the detainees and “overnight we got exponentially...more accuracy in our targeting and applied it on the battlefield in a digital flash.” Flynn also started to realize that the world of open source media was becoming more and more useful—and would earn more dividends later on with the rapid rise of social media.

Flynn does not underestimate his enemies, and admits that many of the terrorists could never be counted on to convert, adding, “Lots of them were gifted fakers... They fooled a lot of us, me included.”

General Flynn’s global strategy is outlined with zeal and precision, but up to this point it lacks any military or governmental will or any type of national or world consensus. In fact, the authors’ urgings resemble the “just-trust-us” neocon scare of the WMD era, but Americans and their nominal allies such as Great Britain are not so trusting this time. Flynn and his writing partner—the longtime anti-communist and vintage neocon Michael Ledeen—will need a much weightier argument than contained in the 194 pages of this slim manifesto before they can get the world to commit to the generations of continual warfare they seek in order to subdue our jihadist enemies, discredit their ideology, create a new set of alliances, and directly confront any regimes that even indirectly support our enemies,

The authors mince few words. “We’re not allowed to say ‘Radical Islam’ or ‘Islamists.’ That’s got to change... Once we’ve understood them, we’ve got to destroy them. It’s not cheap and it’s probably going to last through several generations.”

.....

### ***BACK CHANNEL TO CUBA: THE HIDDEN HISTORY OF NEGOTIATIONS BETWEEN WASHINGTON AND HAVANA***

William M. LeoGrande and Peter Kornbluh.

Chapel Hill: University of North Carolina Press. 2014.

544 pages.

**Reviewed by Jaime González and Dr. David R. Lessard. Mr. González is a senior intelligence officer at the Defense Intelligence Agency. Dr. Lessard is former director of the Western Hemisphere Research Initiative, Center for Strategic Intelligence Research, National Intelligence University, and earlier the Defense Intelligence Officer for Latin America.**

**[Reviewers’ Note: All statements of fact, analysis, or opinion are those of the authors and do not reflect the official policy or position of the National Intelligence University, Defense Intelligence Agency, the Department of Defense, or the U.S. Government.]**

**W**illiam LeoGrande, Professor of Government at American University, and Peter Kornbluh, Director of the Cuba Documentation Project at the National Security Archive at George Washington University, have written an engaging, superbly sourced, and useful book titled *Back Channel to Cuba: The Hidden History of Negotiations between Washington and Havana*.

Publication of this book occurred at a propitious time. In December 2014, the United States and Cuba announced their countries would restore diplomatic ties, and in 2015 Cuban President Raúl Castro participated for the first time in the Summit of the Americas meeting of heads of state. The book demonstrates that, since 1959, each U.S. President and Cuban leader Fidel Castro masterfully used veiled diplomatic communications commonly known as back-channel diplomacy to try to reestablish normal relations, despite persistent acrimonious conflict. We recommend this book not only for its contributions to the historical record of U.S.-Cuban diplomatic relations, but also for its usefulness in guiding analysis of the new efforts to reconstruct bilateral relations.

This is a well-researched book. The authors spent a decade-plus of digging through classified documents obtained through the Freedom of Information Act and

mandatory declassification review, as well as archival research at Presidential libraries and academic institutions. The narrative is enriched by personal interviews of key protagonists and antagonists in the diplomatic drama.

Some heretofore unknown details about key events are revealed. Just before the OAS vote in 1964 to suspend Cuban membership, the U.S., Brazil, and Mexico made a “secret pact” that one Latin American country—Mexico—would maintain ties to Cuba. In 1974 then-Secretary of State Henry Kissinger opened the most serious effort to normalize relations since the Cuban Revolution, despite opposition from President Richard Nixon, but Fidel Castro’s decision to deploy troops to support independence fighters in Angola in 1976 turned Kissinger apoplectic, prompting consideration of acts of war—mining harbors or airstrikes—against selected Cuban targets.

given the loss of Soviet aid and economic distress in Cuba. In any case, the NIE effectively provoked a policy debate about how the U.S. should respond to social collapse in Cuba.

Analysts can take away a few lessons from this book. First, even though information obtained through back-channel diplomacy and related documents probably was out of reach of both policy and intelligence analysts at the time, it is important for analysts to be knowledgeable about current U.S. policy and how it fits into the history of U.S. foreign policy regarding a particular nation. This book provides context about the history of U.S.-Cuban diplomatic relations. Second, analysts should use the lessons of hindsight from this book to understand areas of potential gains and setbacks as both countries embark on yet another effort to reach cooperation and reconcile differences.



***THE LOCKWOOD ANALYTICAL METHOD  
FOR PREDICTION (LAMP): A METHOD  
FOR PREDICTIVE INTELLIGENCE  
ANALYSIS***

Jonathan S. Lockwood.  
New York, Bloomsbury. 2013.  
272 pages.

**Reviewed by Dr. John D. Sislin, a geospatial analyst at the National Geospatial-Intelligence Agency. He is currently on a joint duty assignment at the National Intelligence University where he focuses on analysis and collection. He received his PhD in political science from Indiana University.**

9/11 and the case of WMD in Iraq were two watershed moments, which among other things precipitated a substantial amount of reflection both inside and outside the Intelligence Community regarding how analysts do their jobs and whether the analytic process can be improved. Such introspection is not new, of course, but it has led to renewed attention to the analyst's toolkit. In that vein comes Jonathan Lockwood's recent book, *The Lockwood Analytic Method for Prediction (LAMP)*, which offers analysts a different approach to assessing possible futures. Because this book presents a new method for analysts, it is worthwhile to examine the process step by step to illuminate the advantages and challenges which an analyst might face in applying the method. Overall, while such application demands significant time and information from an analyst, the rewards may be realized through improved collection and organization of information, a better framework in which to cast the problem under study, more thorough identification of relevant actors and their actions, and the consideration of alternate possible futures and the determination of which futures may be more likely.

The book itself has a logical flow and is well organized. The first half of the book focuses on the theory of the method. It describes the process of LAMP, compares the method to four other commonly used techniques (the Analytic Hierarchy Process, or AHP; the Delphi Technique; Alternative Futures Analysis; and the Analysis of Competing Hypotheses, or ACH), presents an illustrative case concerning a reexamination of the author's early work on the former nuclear Soviet republics, and concludes with a discussion of the limitations and applications of the method. The second part of the book introduces three illustrative cases focusing on the future stability of Afghanistan, future conflict between Hezbollah and Israel, and possible future actions by the FARC and ELN—two guerrilla groups—in Colombia. As Mark Lowenthal, a noted scholar of intelligence studies, writes in the introduction to the book, comparing methods and noting limitations is an important

and useful exercise. The four case studies, including the author's own reexamination, illustrate the method in practice and are informative in their own right as important topics in international affairs.

This reader would have appreciated additional discussion about current analytical failings at the outset of the book. Perhaps it is just taken for granted at this point in time that analysis is far from ideal and analysts can do better. However, a discussion early in the text could help frame the discussion in Chapter Two when Lockwood asks: "Why use this particular predictive analytical method when there are other established analytical techniques that have demonstrated merit?" (p. 23) This is an important question. Lockwood provides two answers. First, he notes that the method is "fundamentally different" and a "potentially more powerful way of analyzing and utilizing existing information to make realistic assessments of the possible alternate futures of any given situation" (p. xiv). On page 4, Lockwood notes LAMP "is designed to give the analyst a more powerful method for organizing all available information." Second, Lockwood suggests that following the steps in the method is designed to help an analyst "avoid a range of analytic fallacies." Lockwood identifies four types of analytic fallacies:

1. **The Enemy** (who can create error through either successful deception or concealment of his intentions and capabilities).
2. **The Analyst** (who can fall victim to one or more analytical fallacies in an attempt to derive actionable intelligence).
3. **The System** (which can create the conditions for strategic surprise through either impeding the process of timely warning or rendering the conclusions of analysts so vague as to be useless to the policymaker).
4. **The Policymaker** (who can become a source of error by unduly influencing the intelligence process in an effort to find support for his or her chosen policy) (p. 18).

It is less clear, though, how using LAMP would be helpful against these fallacies. In the case of successful deception or concealment of an enemy's intentions, it would seem likely that the analyst could form an incorrect description of the perceptions of important actors or an incomplete idea of an actor's potential actions. While the analyst may be more thorough, the method also does not seem to inherently diminish the possibility for an analyst's own cognitive failings, such as biases, misuse of heuristics, groupthink, etc. However, Lockwood does suggest that successfully completing Step 3, where each actor's perceptions are described, may help the analyst avoid "mirror imaging," or substituting the analyst's logic for the actor's. Finally, all



analysts, regardless of the method they employ to produce their analysis, face the risk that their analysis will be altered, watered down, ignored, misinterpreted, etc., by more senior analysts, editors, or policymakers.

This said, the method can be helpful in getting analysts to apply a structured technique to their work and to more comprehensively identify alternatives and then organize and manage information. Moreover, LAMP certainly has a wide range of applications. Lockwood notes that practically any issue can be framed in a way to be subjected to LAMP and in Chapter Four suggests several possible ways to apply the method, such as: for indications and warnings (I&W); to carry out long-range intelligence estimates; potentially for diagnostic and evaluative applications; as a training device useful in classroom settings; and as a means to refine other structured analytic techniques.

### Examining the Method

Returning to Chapter One, Lockwood lays out the LAMP method, which involves 12 steps:

1. Determine the issue for which you are trying to predict the most likely future.
2. Specify the national “actors” involved.
3. Perform an in-depth study of how each actor perceives the issue in question.
4. Specify all possible courses of action for each actor.
5. Determine the major scenarios within which you will compare the alternate futures.
6. Calculate the total number of permutations of possible “alternate futures” for each scenario.
7. Perform a “pair-wise comparison” of all alternate futures within the scenario to determine their relative probability.
8. Rank the alternate futures for each scenario from highest relative probability to lowest based on the number of “votes” received.
9. Assuming that each future occurs, analyze each alternate future in terms of its consequences for the issue in question.
10. Determine the “focal events” that must occur in our present in order to bring about a given alternate future.
11. Develop indicators for the focal events.
12. State the potential of a given alternate future to “transpose” into another alternate future.

### Comments on the Process

In Step 1, the user is charged with articulating the issue in the form of a question to be studied. Lockwood notes the range of questions that can be asked is extremely large, which is a positive attribute of this approach. He correctly

cautions against overly vague or broad questions and to frame the question in a way that brings in a limited number of actors and actions. Coming up with good questions can be difficult for analysts, students, and scholars, and forcing an analyst to spend some time thinking about this prior to launching into efforts to solve the question is worthwhile and can help an analyst wasting his/her time and effort on a poor, misguided, or insignificant question.

In Step 2, the national “actors” are identified. The quotes, as Lockwood explains, refer to the notion that to be an actor one must be able to take actions—not everyone is involved in every issue. If one has framed the question appropriately, an analyst should identify no more than five or six actors. The ability to analyze different types of actors is a positive, though this step is one example where the method has a tendency to be reductionist. Three examples are: focusing on a small number of actors, portraying the actors as unitary, and focusing on actors that have a direct effect. Whether simplification hurts or helps analysis is debatable; regardless, it can be challenging for an analyst. For example, how might one reduce the number of actors in a situation such as international trade agreements or arms control efforts? Different analysts might derive different solutions. Treating actors as unitary runs the risk of not explicitly considering the potential wealth of information (at least for some actors) concerning the effect of politics and decision-making on an actor. Finally, selecting actors who have a direct effect is a process that could also vary by analyst, who might have different ideas of who is most relevant. For example, Chapter 5, which focuses on possible futures in Afghanistan, excludes Pakistan as an actor, while Chapter 6, which focuses on interactions among Israel, Hezbollah, and the U.S., excludes Iran. This is not meant to imply that the actors used are wrong or right, but rather that there might be more than one idea regarding which actors are relevant. Different solutions to the question “who matters?” are likely to produce different alternate futures and different rankings of which futures are most likely.

Step 3 focuses on understanding the perceptions of each actor identified above toward the issue the analyst is studying. This is one of the steps that demands the most effort from the analyst and is likely to be one of the most time-consuming, although rewarding, steps in the overall method. That said, the analyst faces two challenges. First, this is an area where a number of different biases could unintentionally enter the process. An analyst might not have complete or correct information. Different pieces of information may be more or less credible. A solution is for the analyst to be explicit about what evidence drives his or her assessment of each actor’s perceptions and whether any evidence was weighted due to such concerns as credibility. Second, this step focuses on perceptions and not on preferences. Actors have perceptions about how the world

is or works, which may or may not be correct. In addition, actors have preferences about how they would like the world to be. These perceptions and preferences cause actors to choose certain actions over others, actions which they hope will lead to their preferred future among various alternate futures. An actor knows its perceptions and preferences and it may guess at, with varying degrees of accuracy, those of its allies and adversaries.

Step 4 focuses on the actor's actions. Lockwood notes that the analyst should include likely and unlikely courses of action, but not impossible ones. This advice suggests that the actions should be collectively exhaustive (the actions cover the range of possible actions and at least one of them has to occur). This is certainly sound advice and may help an analyst think more thoroughly about the range of possible actions. For the sake of parsimony, one could aggregate similar actions together, as long as the analyst feels they are not meaningfully different. For example, limited attacks undertaken by fighter aircraft, bombers, armed drones, cruise missiles, or artillery could all be thought of as a limited military strike.

Many of the examples in the book display symmetry in terms of the actions (e.g., each actor can take the same actions). This may not always be the case and the analyst needs to be careful to recognize that, particularly when the actors are not symmetric—such as a great power versus a minor power, or a state versus an insurgent group, one actor may have a lot more options open to it than another. Second, there is the issue that you are sort of reducing an actor to performing one action, but not multiple actions simultaneously. For example, a state might apply sanctions on another country at the same time it is negotiating with it—or just one or the other. Again, I think that the real world is quite complex and this raises the question of whether this method on its own best captures that complexity.

In Step 5, the analyst determines the major scenarios within which alternate futures are compared. As Lockwood notes, a “scenario provides the major assumptions that will influence the actions of all national actors concerned for that predictive issue.” I think this is an important step, but I am left wondering how an analyst should determine how many scenarios there are and what forces create different scenarios. In the case study of the former Soviet nuclear republics, there were four scenarios based on the interaction of two factors: the success or failure of the Russian government in gaining control over the nuclear weapons, and the collapse or recovery of the economies of the republics. The challenge for an analyst will be to identify the major assumptions in a parsimonious way. For example, consider the hypothetical consequences of North Korea obtaining a nuclear arsenal. Military factors might include whether or not North Korea can miniaturize a warhead, whether or not it has a ballistic missile, and whether it is a fission or fusion device. Additionally, though, one can

imagine political drivers, such as Kim Jong-un's control over the leadership (strong or weak), or economic drivers, such as the state of the economy (doing well or doing poorly). The analyst will have to figure out which dynamics are most important to create scenarios and then justify those choices.

Steps 6 to 9 focus on creating alternate futures for each scenario, next performing a pair-wise comparison of these futures to determine which are more likely, and then analyzing each future in terms of its consequences. For example, if we assume there are three actors and three choices, as for example in the case study in Chapter Six, where the three actors are Israel, the United States, and Lebanon and the three choices open to each of them are diplomatic engagement, limited response, and full response, then there are 27 possible combinations created. All three actors may attempt diplomatic engagement, two of the three actors may do so, one of the three actors may do so, or none of the actors may do so, and so forth. For purposes of LAMP, the 27 combinations are termed “alternate futures.”

In this portion of the process, an analyst is likely to face several challenges. The most important issue is that, in judging the likelihood of each alternate future compared with the others, the evidence for making such assessments remains implicit. As Lockwood notes, the evidence is based on the analyst's current knowledge of the actors and their perceptions. Where one finds such evidence, how one aggregates different and possibly contradictory pieces of evidence, and how one weights the evidence, is up to the analyst. This part of the process is not transparent. For example, while the case studies in the book show ranked lists of futures, it is unclear how votes actually occurred. I think this is a serious challenge for an analyst using this method in defending whatever answer is resultant and for other analysts to be confident in the results because they are able to replicate them. A simple solution would be to incorporate a numbered list of the evidence with a matrix reflecting which pieces of evidence favored which future in each pair. However, a related point is that the analyst needs to work through a lot of comparisons. For three actors with three actions, there are 351 comparisons that need to be made. This constitutes a large number of analytic judgments and is a place where an analyst's biases might enter.

Steps 10 to 12 focus on identifying “focal events” that must occur in our present in order to bring about a given alternate future. Lockwood describes these focal events as akin to a fork in the road at which point actors are heading toward one future and away from another. From these focal events, indicators can be developed. The indicators are signs that the focal event is more likely. These are things that can be used in the future as I&W or to reassess the situation in light of new developments. This is an advantage of the method. In the final step, the analyst should state the

Overall, this book is an important contribution to the discussion of how analysts approach their work, what tools they can use, and the benefits and disadvantages of using each tool. Lockwood does an excellent job of presenting an impartial elaboration of the method and offers four different examples of the method in practice. Encouraging the use of a structured technique is a positive approach and asking analysts to be clear about their research question and the elements that comprise it—the actors, their views, and their actions—is promising.

I raise two general issues, which I think can be overcome, with greater explicitness or by adding additional steps. Procedurally, the most important issue for this reader is Step 7. How the voting is conducted remains too much of a mystery, more in the mind of the analyst, for my comfort. This could create challenges for others to replicate the analysis. In addition, the method is designed to increase the range of outcomes resulting from the interaction of the different actions taken by all actors. Yet the method does not appear to consider explicitly the actors' preferences, which ought to play a large role in determining which futures are more likely. Including a discussion of each actor's preferences at the same time as looking at his/her perceptions may be helpful.

A second issue is that the method asks a lot of the analyst. First, the approach requires a lot of time, information, and effort and thus would be more difficult for quick turnaround intelligence problems. Likewise, describing the elements of LAMP—especially the actors' perceptions, the scenarios, and the alternate futures—is more amenable to a longer product, which may be a burden on policymakers. For students or scholars, this is not necessarily a problem, though for any analyst under time constraints this approach might be best utilized for long-term, larger research projects, where a lengthy report is appropriate. Second, the analyst is often unlikely to have enough information to fully describe actors' perceptions and evaluate pair-wise comparisons. One solution is to more explicitly identify the evidence used and also missing evidence or limitations of the evidence (e.g., dated evidence of uncertain credibility). That would increase transparency and make the process more replicable. A lot of the actual analysis is implicit. Third, there is no built-in mechanism to prevent analysts from doing it incorrectly.

In conclusion, I find LAMP to be a useful tool, if applied with as much transparency as possible. Providing the

evidence and linking it to the outcomes of the pair-wise comparisons could be helpful. Likewise, adding some analysis of actors' preferences, not just their perceptions, could also be of benefit. This method would be most applicable for long-term studies on particular problems. It joins a number of other techniques designed to help analysts be more structured, organized, and open-minded to a range of possible outcomes.



## Peter Caddick-Adams.

Oxford, UK, Oxford University Press. 2013.  
396 pages.

**Reviewed by Harry L. Petrey II, who has 22 years of federal service and currently works as an intelligence specialist for the Department of the Navy at the Pentagon. He graduated with a master's degree from the National Intelligence University in 2013, previously was a student in NIU's undergraduate program, and is a charter member and officer of the NIU Alumni Association. His grandfather, LTC Maurice E. Peabody, was an Army company commander serving in the campaigns covered in this book.**

The Pacific and European campaigns dominate modern retelling of the war fought by our “Greatest Generation.” Little fanfare is given to the trials of the men who won a key, yet costly, Allied victory in Italy. Amid strategic preparations for the landings at Normandy, and after the Axis defeat in North Africa, Allied leaders turned their attention to outmaneuver the German *Wehrmacht* by assailing the fortifications spanning the Italian peninsula and taking Rome. Monte Cassino is the retelling of this campaign by Peter Caddick-Adams. He offers, in heartbreaking detail, a near encyclopedic retelling of the battles to break the German defensive lines.

Caddick-Adams begins with important motivations of the Allied combatants, along with their experiences in North Africa and the landings in Sicily. This sets the stage for grievous failures derived partly from an over-reliance on technology—a theme all too relevant in modern times. The author goes on to provide keen insights into the leaders of the opposing armies. Field Marshal Albert Kesselring, a contemporary of the more famous “Desert Fox,” Field Marshal Erwin Rommel, leads the Reich’s Mediterranean forces. Kesselring gives both his generals, Heinrich von Vietinghoff and Fridolin von Senger, great latitude to serve as able and reliable field commanders.

## BOOKSHELF

Interesting differences in leadership styles are emphasized by Caddick-Adams' retelling of the German lines in Italy. German officers were expected to take command of higher and lower echelons as necessary and were more decisive during the dynamics of warfare. This was often a factor in neutralizing the Allied advantage. The Germans were able to thwart Allied air supremacy and materiel superiority in spite of Allied decryption of communications from Berlin to Kesselring's headquarters. The Allied Mediterranean Theater Commander, Field Marshal Harold Alexander, once quipped the Germans were "above all quicker at reaching decisions on the battlefield. By comparison our methods are often slow and cumbersome."

Alexander contended with U.S. General Mark Clark and British General Oliver Leese. Although on the same side of the conflict, Clark and Leese seemed to be fighting separate and coincident battles. Caddick-Adams suggests Clark unsuccessfully split his attention between the Anzio beachhead and his front on the Gustav Line while Leese remained distantly concerned with his command. Both are described as failing to capitalize on discrete tactical advances by not directing reinforcements from each other to press the advantage. These trends contributed to Alexander's lack of demonstrated successes, which conspired with the weather, and resultant lack of air cover, to prolong the campaign from mid-January to mid-May 1944.

Of the ten armies, the British and U.S. commanders held the most senior positions, but Caddick-Adams provides additional perspectives from the Italian, French, and other contributors to allow full appreciation of the attempts to take Monte Cassino. One description illuminates the horrible winter of 1944. Weeks of rain engorged rivers and turned roads to mud. Weather and terrain made Allied armor all but useless. Infantrymen slogged through muck, reminiscent of trench warfare. Snow and ice made the steep and narrow trails almost impossible to navigate, especially when under fire. Another account expresses the significant, albeit unanticipated, contributions made by the local Italians. *Salmere*—mule handlers—and their mules became essential logistical resources for the infantry. *Salmere* carried ammunition, food, and supplies and evacuated casualties where a motor transport could not. Similar contributions came from the Moroccan-French units. Their mountaineering expertise, along with support from the *Salmere*, enabled the advancement against the well-fortified German positions, despite incurring heavy casualties.

Caddick-Adams skillfully conjures up the tensions among Allied plans of action. The valor and missteps of the leaders is shown through their efforts to draw support

from Italy, delay the landing in southern France, and prepare for the landing at Normandy. He describes Churchill's urgent gambit to draw reserves from the Gustav Line. Churchill hoped to establish a beachhead at Anzio and flank the Germans. Caddick-Adams tells of Clark's tenuous efforts to hold Anzio while pressing toward Rome. He goes further to depict the Pyrrhic attempts by the Polish, Moroccan-French, Italian, Greek, Indian, and U.S. forces to take the linchpin of the campaign—Monte Cassino.

The author made several trips to Monte Cassino, the rebuilt monastery, and other fortifications along the Gustav Line in preparation for his book. His familiarity with the challenging terrain is expertly explained in this account. His position as a lecturer at the United Kingdom's Defence Academy is also evident. Some readers' tastes may not be suited to the author's style, which often requires recalling logistical details, order of battle specifics, and volatile relationships. This book not only speaks to modern themes of soldiers pushing through adversity in spite of what they lack but also evokes fond appreciation for the Greatest Generation and its lessons still to be learned. Monte Cassino provides surprising insights into coalition warfare from six decades past that can still inform contemporary doctrine. Peter Caddick-Adams' retelling of the Italian campaign is a lively and talented narrative that calls to mind the heart and soul of the struggle undertaken by brave souls fighting in a forgotten theater of the war.

.....

**Submit a book for review!**

**Please send copies to:**



**American Intelligence Journal  
256 Morris Creek Road  
Cullen, Virginia 23934**



## Review Essay: Spy Ships and the Collection of Signals Intelligence

### ***THE LIBERTY INCIDENT REVEALED: THE DEFINITIVE ACCOUNT OF THE 1967 ISRAELI ATTACK ON THE U.S. NAVY SPY SHIP.***

A. Jay Cristol.  
Annapolis, MD, U.S. Naval Institute. 2013.  
416 pages.

### ***ACT OF WAR: LYNDON JOHNSON, NORTH KOREA, AND THE CAPTURE OF THE SPY SHIP PUEBLO.***

Jack Cheevers.  
New York, Penguin. 2013.  
448 pages.

### ***THE PUEBLO INCIDENT: A SPY SHIP AND THE FAILURE OF AMERICAN FOREIGN POLICY.***

Mitchell B. Lerner.  
Lawrence, University Press of Kansas. 2002.  
320 pages.

---

**Reviewed by LTC (USAR, Ret) Christopher E. Bailey, a faculty member at the National Intelligence University specializing in national security law, processes, intelligence ethics, and strategy. He is a 2008 graduate of NIU's Denial & Deception Advanced Studies Program and the U.S. Army War College. He is licensed to practice law in California and the District of Columbia, and is a member of the National Security Law Section, American Bar Association. He is a candidate for the LLM degree in National Security & U.S. Foreign Relations Law at the George Washington University School of Law.**

[Reviewer's Comment: The opinions expressed in this article are the reviewer's personal ones and do not imply endorsement by the National Intelligence University or the Defense Intelligence Agency.]

Several recent books illustrate important policy, legal, and moral/ethical issues involving the use of ships to collect signals intelligence (SIGINT) in or near conflict zones. In *The Liberty Incident Revealed*, former naval aviator and federal judge A. Jay Cristol provides a detailed examination of Israel's controversial June 8, 1967, attack on the USS *Liberty* that left 34 dead, many of whom were employees of the National Security Agency (NSA). Cristol's work is actually an update of his earlier book, *The Liberty Incident*<sup>1</sup>; the new edition includes recently declassified intercepts made by NSA concerning transmissions between Israeli Air Force pilots and air traffic controllers. In *Act of War*, former political writer Jack Cheevers chronicles the

story of Commander Pete Bucher and his crew who were held by North Korea in an 11-month ordeal that started with their capture on January 23, 1968, near the port of Wonsan. Cheevers offers a fast-paced, engaging narrative focused on Bucher and his crew, who suffered a long ordeal involving harsh interrogations, torture, and mistreatment by an enemy who would not extend any rights to the prisoners under the 1949 Geneva Conventions.<sup>2</sup> Nonetheless, historian Mitchell Lerner's 2002 book *The Pueblo Incident* likely remains the overall, definitive account of that political-military crisis between the United States and North Korea. Each book has benefited from a wealth of formerly classified and open source documents, extensive interviews with participants, and detailed analysis; each book offers important lessons for intelligence practitioners and policymakers.

Lerner provides an excellent history of the U.S. spy ship program, noting that NSA started the initiative in 1960 and patterned it on the Soviet program that had been sending spy ships (actually disguised as fishing trawlers) to surveil the American coast and trail ships at sea. Eventually, the joint NSA-Navy effort expanded to seven ships, to include the USS *Liberty* (AGTR-5), but all under NSA control. By 1965, however, the Navy was dissatisfied with its lack of control over the ships and their mission assignments, and it proceeded forward with a new plan to establish a fleet of 30-70 boats dedicated to the collection of SIGINT for its own use. The first phase of this program led to the use of a single ship to serve as the prototype; three ships were commissioned in this class, the USS *Banner* (AGER-1), the

USS *Pueblo* (AGER-2), and the USS *Palm Beach* (AGER-3). It was the two short cruises, neither armed since early 1967, made by the USS *Banner* in the Sea of Japan and the East China Sea that provided the model that led to the ill-fated first and only cruise of the USS *Pueblo* as a spy ship.

The spy ship program operated under several important assumptions. First, the Soviet Union had been surveilling the American coast and trailing U.S. ships for several years, and its spy ships had not been attacked by the United States. NSA and the Navy reasoned, in a like manner, that their spy ships could surveil the Soviet coast and its ships without being attacked. Second, the United States believed that its spy ships were protected by international law, as long as they stayed outside the 12-mile territorial limit claimed by most communist nations. Third, as Lerner examines, U.S. policymakers and intelligence practitioners had a mindset bias, believing that the North Koreans were serving broader communist interests as opposed to a people with its own nationalist agenda. In overall terms, this led to a situation in which the U.S. Navy failed to anticipate some of the problems that the spy skippers like Commander Bucher might face. Also, in the case of Bucher and his crew, the mindset bias hindered policymakers who were slow in grasping what was needed to resolve the standoff and secure the crew's release. In any case, Navy planners and policymakers, when preparing for the *Pueblo* and *Liberty* missions, could have benefited from careful consideration of several lessons that should have been learned from the 1964 experiences of the USS *Maddox* and the USS *C. Turner Joy* in the Gulf of Tonkin.

In early 1964 the United States had been supporting a series of South Vietnamese covert (OPLAN 34A) raids against the North Vietnamese coast of the Gulf of Tonkin. Here, Edwin Moise gives a detailed examination of the August 1964 incidents involving the two destroyers; this offers a useful basis of comparison with the later 1967 *Liberty* and 1968 *Pueblo* incidents.<sup>3</sup> One important difference centers on the fact that both the *Maddox* and the *Turner Joy* were destroyers, with the *Maddox* carrying communications intercept equipment. With such ships, the communications equipment/specialists were typically on board to support the ship's captain with his own mission. However, with the spy ships, sometimes thinly disguised as oceanographic research vessels with minimal defensive armament, the captain's role was to support the intelligence collection mission and the needs of his on-board collectors. Indeed, the movement of a combatant vessel with five-inch guns, like the *Maddox* on a DeSoto patrol, sometimes operating within the 12-mile territorial limit of the North Vietnamese coast and near in time/location to the South Vietnamese maritime raids, could readily be seen by Hanoi as an inherently provocative act.<sup>4</sup> It is hardly surprising that three North Vietnamese motor torpedo (PT) boats might sally forth on August 2,

1964, even though the *Maddox* was actually in international waters at that time (probably 28 nautical miles from the coast).<sup>5</sup>

The 1967 *Liberty* incident illustrates some of the recurring problems that occur in war. While responsible combatants readily grasp the basic moral/legal principles under international humanitarian law involving necessity,<sup>6</sup> distinction,<sup>7</sup> and proportionality,<sup>8</sup> the application of those targeting principles under the pressures of modern combat can be difficult. Here, Judge Cristol combines the experience of a former naval aviator and the lawyer's appreciation for the meaning and interpretation of evidence, including gun camera film and post-flight debriefing reports, to show how the serial mistakes of the U.S. Navy, the Israeli Air Force, and the Israeli Navy left the ship in a vulnerable position that was easily mistaken for an Egyptian ship. Judge Cristol provides a masterful analysis that shows how and why this friendly fire incident came about. While conspiracy theorists probably will not be satisfied, Judge Cristol makes persuasive case that—barring radically new evidence—the tragic incident was the result of mistaken identity, not an intentional attack by an ally.

The *Liberty* incident is also a good illustration of the long-standing tension between maintaining secrecy about an intelligence activity and the need for transparency/public accountability. Here, the lack of transparency on the part of the administration was a contributing factor in bringing about the Israeli attack, and it also complicated the administration's efforts to ensure post-attack accountability. Neither the Pentagon nor NSA had informed the U.S. Embassy in Tel Aviv or the Israelis about the planned activities (e.g., identification and general operating areas) of the ship; in fact, the U.S. government had earlier (on June 6) announced that it had no ships in the area. Indeed, the Spanish government was concerned that the misleading word that the ship had sailed from Rota might be seen by Arab governments as supporting Israel in the ongoing Six Day War. Finally, after the attack, the administration's lack of candor, to include the long delays in releasing NSA intercepts and government reports, about the ship's mission only fueled the speculation and debate about the ship and what had actually happened.

The 1968 *Pueblo* incident offers an excellent case study in a range of strategic issues. Initially, the Johnson administration faced three important questions: it did not know the ship's actual location at the time of seizure, it did not know how the decision to surrender came about (CDR Bucher had orders to avoid any appearances of a hostile act), and it did not know the extent of the intelligence loss. President Johnson also faced three conflicting foreign policy imperatives: he wanted to obtain a speedy return of the ship's crew, he wanted to maintain South Korea's

commitment to the fight in South Vietnam (it had two infantry divisions deployed there) and, with rising tensions between North and South Korea, he wanted to avoid another war in Asia that could entangle the United States. While the Johnson administration tried different diplomatic approaches with North Korea, to include soliciting assistance from Moscow or taking the matter to the United Nations Security Council, the North Korean negotiators remained steadfast in their “three A’s demand.” Kim Il-sung demanded that the United States admit to violations of North Korean sovereignty, apologize for its actions, and assure North Korea that it would not commit any such acts again in the future. President Johnson evidently did take one lesson from the 1964 Tonkin Gulf incident; he showed considerable restraint in the face of strong calls for a military response from his conservative critics and South Korean President Park Chung-hee. President Johnson examined numerous post-seizure options for freeing the crew or mounting reprisals against North Korea, but no option appeared to have any realistic chance of success. In the end, Johnson’s willingness to endure the longer agony, both for the nation and the crew, of protracted and often exasperating negotiations probably saved lives and helped prevent renewed war on the peninsula.

Lerner provides a tour de force with his in-depth analysis of the prevailing liberal international view (the foreign policy paradigm that American security could only be guaranteed by a determined opposition to the spread of communism on every front), and the deeply-held nationalist and ideological views of the North Korean leader. In his opinion, the U.S. failure to overcome the narrow assumptions about the nature of the Cold War was the “largest contributing factor in the seizure” of the ship, and also hindered later resolution of the crisis.<sup>9</sup> Lerner expertly examines *juche* (the North Korean self-reliance ideology) from political, economic, and military perspectives; he shows how Kim Il-sung acted for domestic political needs and left President Johnson with no choice but to secure the prisoners’ release by meeting the “three A’s” demand in some form. Finally, he shows how a lack of transparency by the Johnson administration on a range of issues (e.g., the *Liberty* incident, Vietnam, and the *Pueblo*’s mission) actually undermined the President’s support by the American people. [Editor’s Note: For more on the *juche* concept, see Dr. David Shin’s article on North Korean leadership in this same volume.]

It is clear from Lerner’s study that mission planners should have considered the provocative nature of the mission from the North Korean point of view. With the *Pueblo* incident, there had been ample recent evidence of North Korean bellicosity, to include a 1965 attack on a U.S. reconnaissance aircraft flying 50 miles east of Wonsan, the ongoing seizures of South Korea fishing boats operating off the North Korean coast (20 boats in the three months before the *Pueblo*

cruise), a January 11, 1968, warning about countermeasures against U.S. “spy boats,” and an attempted assassination of the South Korean president on January 21, 1968 (the Blue House raid by a platoon of 31 North Korean commandos).

Lerner examines the need for a rigorous risk assessment process at various levels, to include consideration of the results of prior missions, the sensitivity and political climate in the area, the nature and scope of the intelligence tasks, the territorial limits, the overall capabilities of the ship, the weather conditions, and the Navy’s ability to provide timely support. He argues that a more complete risk assessment would have yielded a different benefit/risk assessment. In fact, Bucher’s superiors might have reconsidered the wisdom of the mission itself or, at a minimum, should have provided for immediately responsive, on-call air support. Second, the ship must be prepared to defend itself or request immediate assistance; neither the *Liberty* nor the *Pueblo* were prepared in that way. Third, if a spy ship is to operate near the territorial limits in a volatile region (e.g., 15 nautical miles by at least one account), it obviously cannot have an unreliable steering engine, much less inexperienced navigators and linguists. Finally, a spy ship loaded with sophisticated, classified equipment and documents must have a ready means of destroying the same, especially if operating in shallow coastal waters.

The 1968 *Pueblo* incident also illustrates some of the moral/ethical problems facing a ship’s captain. CDR Bucher reached a point at which he was confronted with greatly superior combat power, facing a situation in which he could either surrender his ship or fight against overwhelming force and see the needless killing of his crew.<sup>10</sup> Bucher, despite his best pre-deployment efforts to prepare his ship and the slipshod planning by his superiors, was left with a situation in which he could not defend his overmatched ship and did not have reason to expect immediate air support. Cheevers shows how Bucher used various delaying tactics to give his crew time to destroy classified materials and allow for the arrival of air support, but was eventually forced to surrender. Here, his failure to fight on—at least in the eyes of his contemporaries—is probably best characterized as a failure of the warrior “ethos”; he became the first U.S. naval commander to surrender his ship without a fight since the 1807 capture of the USS *Chesapeake* by the British off Cape Henry, VA.<sup>11</sup> In that sense, Bucher acted contrary to the long-standing and deeply cherished naval tradition in the mold of John Paul Jones (capturing the *Serapis* after his own ship sank), Stephen Decatur (fighting the Barbary pirates from 1801 to 1804), and the last, revered words of James Lawrence during an 1813 battle that were emblazoned on a banner which hung at the U.S. Naval Academy for generations (“Don’t give up the ship!”).

The U.S. government's treatment of CDR Bucher and his crew, especially as compared to the earlier recognition received by CDR William McGonagle and the *Liberty* crew, is astounding. Initially, the Navy informed families of their loved ones' internment by mimeographed letter. In fact, neither President Johnson nor any of the senior Navy leaders ever actually called or tried to maintain contact with the *Pueblo* families. Moreover, when Rose Bucher tried to get contact information for the other *Pueblo* families, the Chief of Naval Personnel rebuffed her, citing the "privacy" interests of those families. After CDR Bucher's release from captivity, the Navy convened a court of inquiry,<sup>12</sup> which recommended a court martial for CDR Bucher and LT Stephen Harris (the former chief of the communications detachment).<sup>13</sup> The Navy did, however, award the Legion of Merit to the legal advisor to the court of inquiry. Eventually, Secretary of the Navy John Chafee overruled the court martial recommendations, at least in part because the failures were shared by Bucher's superiors and possibly because of the public support for Bucher and his crew. Still, after Congress created a Prisoner of War Medal in 1985, the Navy refused to award it to the crew based upon a technical question of whether the crew had been "engaged in an action against an enemy of the United States" (the 1950-53 Korean conflict had ended in an armistice, meaning that North Korea was technically still an enemy of the United States). It was not until 1990 that the award was actually granted after a bitter fight.<sup>14</sup>

On the other hand, CDR McGonagle, who was clearly operating in an area where the United States was not at war, received very different treatment from the Navy. Later-CAPT McGonagle, who had been wounded in the initial attack, received the Medal of Honor for his efforts to defend and save his ship from friendly fire, and the engineering officer—who came aboard after the attack—received the Bronze Star for getting the stricken ship back to port.<sup>15</sup> There is no question that the skipper and engineering officer were decorated for what were undoubtedly gallant and conspicuous acts of heroism in the finest sense of naval tradition. Yet one important reason for the difference in the treatment meted out to the two skippers is probably best summed up by one senior officer: "The decision to clear Commander Bucher ... was good news to many folks including my dear wife, but to me he will always be a coward disgracing our navy and blackening our glorious naval tradition."<sup>16</sup>

There are some interesting intelligence lessons to be learned from these three incidents. The 1964 Tonkin Gulf incidents illustrate some of the recurring problems with intelligence reporting, to include initial reports that are incomplete, ambiguous, or contradictory. In fact, one problem that Moise addresses involves the inaccurate date-time groups on the initial messages sent from the western Pacific, making

it difficult to understand when certain events occurred. The *Liberty* incident shows how the combined errors in intelligence reporting, problems with situation management in a command headquarters, and information available to attacking personnel can lead to tragic consequences. Judge Cristol's fruitful experiences in researching this recent edition demonstrates the continuing value of getting NSA intercepts and document releases through the Freedom of Information Act, as well as the need for access to foreign witnesses and documentation.

The 1968 *Pueblo* incident highlights some of the problems faced by intelligence officers captured by the enemy. Here, both Lerner and Cheevers provide detailed accounts of the Code of Conduct challenges faced by the crew and some of the subtle tactics used by the prisoners as they endured torture and mistreatment. Some tactics, such as the use of the "Hawaiian good luck sign" (an extended middle finger), ultimately humiliated the North Korean jailors, but did give the crew some sense of identity and a means of resistance. Other tactics, such as leaving a urine-soaked apple for a guard who was known for stealing from the prisoners, were remarkably effective. One amusing anecdote involved the crew's confession about violating North Korean waters; the crew—knowing that their captors did not understand navigational issues—prepared a chart that showed numerous impossible violations that at one point put the ship on a mountainside and also had it six miles inland in downtown Wonsan.<sup>17</sup> In any case, it is noteworthy that the North Koreans conducted very limited interrogations of intelligence value, mostly focusing their efforts on points for domestic political (propaganda) gain.

Finally, the United States suffered a devastating intelligence loss with the capture of the *Pueblo*; the ship was loaded with important communications equipment, code books, and documents, only a fraction of which could be destroyed by the crew before capture and most of which were presumably sent to the Soviet Union. In any case, a spy ship must be equipped with adequate equipment to destroy classified equipment and documents in an emergency, and must not be burdened with unnecessary classified material. While the government did conduct an intelligence damage assessment, as well as detailed post-release debriefings of the crew, it obviously did not know that John A. Walker and his friend Jerry Whitworth had already started selling codes and documents to the Soviet Union the year before.

I strongly recommend these books for intelligence practitioners interested in Cold War intelligence operations. Each author has completed thorough, in-depth research, offering important perspectives on the issues.



## NOTES

<sup>1</sup> A. Jay Cristol, *The Liberty Incident: The 1967 Attack on the U.S. Navy Spy Ship* (Dulles, VA: Brassey's, 2002).

<sup>2</sup> North Korea (Democratic People's Republic of Korea, or the DPRK) has been a state party to the 1949 Geneva Conventions, to include the *Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949* (Geneva Convention III) since August 27, 1957.

<sup>3</sup> Edwin Moise, *Tonkin Gulf and the Escalation of the Vietnam War* (Chapel Hill: The University of North Carolina Press, 1996).

<sup>4</sup> The Charter of the United Nations, Article 2(4), provides that "all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." In that sense, the earlier OPLAN 34A raids, combined with the presence of a supporting U.S. destroyer, could have easily justified North Vietnam's inherent right of self-defense under Article 51.

<sup>5</sup> Both the USS *Maddox* and the USS *C. Turner Joy* were involved in the second "incident" that allegedly involved a North Vietnamese attack on both destroyers on August 4. Moise makes a detailed and persuasive argument that the second incident did not occur and that both ships were likely firing weapons at "ghost images." Here, the destroyers had immediate air support from the aircraft carrier USS *Ticonderoga* (CVA-14). It is noteworthy that neither Commander (later Vice Admiral) James Stockdale nor Lieutenant Everett Alvarez (who was shot down and captured during this mission, becoming the longest-held U.S. prisoner during this war), both flying air cover for the destroyers, could find any North Vietnamese vessels that were "attacking" the destroyers. In 1965 CDR Stockdale was shot down and captured by the North Vietnamese; he later received the Medal of Honor after his lengthy captivity. LT Alvarez later graduated from the George Washington University School of Law and in 1982 became the Deputy Administrator of the Veterans Administration. Moise artfully reconstructs this second incident, showing problems with the ship tracking, radar, witness and signals intercept reports. He illustrates how the problems with the initial combat reporting, to include incomplete and contradictory reports, combined with Pentagon leaders bypassing the chain of command in an effort to get badly needed answers, led to faulty decision-making by the President and the Congress. Indeed, one doubts that the Congress would have passed the Tonkin Gulf Resolution, providing domestic legal authority for broad combat operations against North Vietnam, if it had the full facts from the incidents.

<sup>6</sup> According to the International Committee of the Red Cross, "The destruction or seizure of the property of an adversary is prohibited, unless required by imperative military necessity." International Committee of the Red Cross, *Customary International Humanitarian Law, Volume I: Rules*, Rule 50 (Cambridge, 2005).

<sup>7</sup> *Id.*, Rule 1 requires that the "parties to the conflict must at all times distinguish between civilians and combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians."

<sup>8</sup> *Id.*, Rule 14 prohibits attacks in war "which would be excessive in relation to the concrete and direct military advantage anticipated."

<sup>9</sup> Lerner, *The Pueblo Incident*, at 97.

<sup>10</sup> CDR Bucher faced six faster and more heavily armed North Korean boats. He initially tried to leave the area, but took fire

from 57-mm cannons and machineguns, leaving several sailors severely wounded and the ship covered in flames and smoke. His own weapons, three .50 caliber machineguns, were located in an exposed position and were completely inadequate against the attackers.

<sup>11</sup> Lerner points out that in 1815 the USS *President* was surrendered by Stephen Decatur to the British in international waters after a close fight.

<sup>12</sup> The court of inquiry is a fact-finding body; it can recommend, but it cannot impose, punishment. The Navy did impose a legal firewall between the debriefings of the crew and the court of inquiry; each crew member was guaranteed that anything said in the debriefings would not be used against him later in disciplinary proceedings. Cheevers provides detailed information about the court of inquiry, its members (here, five distinguished admirals) and legal counsel, and its proceedings. He explains that the court had a narrow focus, largely limited to the actions of CDR Bucher; the court was prohibited from calling any witnesses higher than Bucher in the chain of command. Unlike the Navy, the House of Representatives impaneled a special subcommittee led by Rep. Otis Pike (D-NY), who led a broad inquiry into the Navy's handling of the *Pueblo*. Cheevers comments that the cantankerous Congressman was no friend of the Navy, noting that he "once killed a bill to give flight pay to deskbound admirals by demonstrating on the House floor how difficult it was to fly a desk." Cheevers, *Act of War*, at 341.

<sup>13</sup> The Navy did, however, award decorations to many of the ship's crew, to include one Navy Cross, two Silver Stars, six Bronze Stars with Combat V device, and nine Navy & Marine Corps Achievement Medals with the Combat V device; all crew members received both the Navy Commendation Medal with Combat V device and the Purple Heart. Only the two Silver Stars were awarded for "conspicuous gallantry and intrepidity in action" on January 23, 1968 (the date of capture); all other awards were made for conduct while in captivity.

<sup>14</sup> The Navy did not even present the awards to the crew; Cheevers explains that the Veterans Administration was put in charge of the ceremony and that it wanted a "neutral" site for the ceremony. Ultimately, the crew received the medal in front of the San Diego County Administration Building.

<sup>15</sup> Like the later *Pueblo* crew, many members of the *Liberty* crew received decorations, to include two Navy Crosses, 11 Silver Stars (three posthumously), 20 Bronze Stars, 9 Navy Commendation Medals, and 204 Purple Hearts.

<sup>16</sup> Lerner, *The Pueblo Incident*, at 227.

<sup>17</sup> This later led one pundit to ask why, if the *Pueblo* had made the purported violations, had the North Koreans not "pulled over" the ship when it had been stopped at a traffic light in downtown Wonsan!

