



1st Quarter 2009

# *THE VANGUARD*

Journal of the Military Intelligence Corps Association



**2009 CSM (R) Doug Russell  
Award and LTC Thomas  
Knowlton Award presented to  
SGT Julian M. Jones**

Volume 14 Number 1

**Publisher**

COL Larry D. Bruns, USA, Retired

**Editorial Office**

P.O. Box 13020, Fort Huachuca, AZ 85670-3020

This issue edited by:

Les Siemens, *Executive Director*

**Email:** vanguard@micorps.org

**Website:** http://www.micorps.org

**Purpose:** *THE VANGUARD* is the official journal of the Military Intelligence Corps Association (MICA) for its members and sponsors. The quarterly journal serves as a professional forum for sharing knowledge, preserving history, and honoring civilian and military members of the Corps.

**Disclaimer:** All rights reserved. The opinions expressed in *THE VANGUARD* are those of the authors and do not necessarily represent the position of the MICA. The content does not necessarily reflect the official position of the U. S. Department of the Army or other U. S. Government organizations.

**Submissions:** Submit articles, photographs, and other material to the Editor, *THE VANGUARD*, at vanguard@micorps.org. Please provide contact information, a description of the material, and a short biography with each submission. *THE VANGUARD* reserves the right to accept, reject, or edit any submissions at its discretion. Articles, photographs, and other material from *THE VANGUARD* may be reproduced, if they are not restricted by law or military regulations, provided proper credit is given and the Editor has given specific prior permission for each reproduced item.

**Change of Address:** Please send your new address along with your old address to administrator@micorps.org or by mail to MICA, P.O. Box 13020, Fort Huachuca, AZ 85670-3020.

**Postmaster:** Send address changes to MICA, P.O. Box 13020, Fort Huachuca, AZ

**Cover:** 3 Mar 2009—CSM (R) Doug Russell congratulates SGT Julian M. Jones and his parents. At the ceremony, held during the annual Military Intelligence Sergeant Majors Conference, SGT Jones was also presented a MICA Knowlton Award by National MICA President, Larry Bruns. (photo by Mark Cline)

# MICA Scholarships

The Military Intelligence Corps Association (MICA) Scholarship Program provides scholarships for individuals pursuing undergraduate degrees or technical certifications. Scholarships may be used for attendance at regionally accredited colleges, universities, or state approved vocational schools/technical institutions.

## Who is Eligible?

Applicants must be a current individual member of MICA or a family member of such. Family members are considered a spouse, children, or immediate relative living with or supported by the qualifying MICA member.

Applicants must be pursuing their first undergraduate (Associates or Bachelors) degree or a technical certification. Applicants already possessing an undergraduate degree or seeking a graduate degree are not eligible.

Previous MICA Scholarship recipients may compete for subsequent scholarships.

## How to Apply

Complete instructions and application forms are located on the MICA webpage at www.micorps.org. Information on MICA membership is also available on this webpage.

Applications must be mailed and postmarked no later than 15 May 2009. Late or incomplete applications will be returned to the applicant without consideration.

## Send completed application to:

Office of the Chief, Military Intelligence (OCMI)  
Attn: MICA Scholarship Chairman  
110 Rhea Street  
Fort Huachuca, Arizona 85613-7080

For more information call: SGM Steven Koroll  
at (520) 533-1174, DSN 821-1174

## Check your mailing label

Please check your mailing label with every issue of *THE VANGUARD*. Your membership renewal date is shown next to your name. You can easily renew online by logging into the member area at www.micorps.org.

The image shows a screenshot of the MICA member area. On the left is a 'LOGIN FORM' with fields for 'Username' (containing 'LSiemens') and 'Password' (masked with dots). There is a 'Remember me' checkbox and a 'Login' button. Below the login form is a 'Lost Password?' link with the text 'A reset login will be sent to your email address.' On the right is the 'MICA MEMBERS' menu, which displays 'Your membership expiration is 01/01/2010' and a list of links: 'Your Information', 'The Vanguard Archive', 'Award Nomination', and 'Contact Mentors'. Three callout boxes provide instructions: 1) 'Using your Username and Password, login for member-only content.' 2) 'If you've forgotten your login details, click the Lost Password link to have them sent by e-mail' 3) 'Once logged in, you will see a MICA Members menu in the left pane; it also shows your membership renewal date.' 4) 'The Your Information link takes you to a form that allows you to view and update your membership contact information, see your expiration date and renew using a credit card online.'

# Notes from the President

Over the last quarter the National Executive Board has undergone significant changes. Bill Morgen has stepped forward to fill the position of Vice President. Bill will focus on membership (individual and corporate) and our Military Intelligence heritage. Those who know Bill understand the dedication and innovation that he brings to all of his endeavors. It is truly an honor to have Bill on the board and we look forward to the numerous contributions he will bring to MICA.

Les Siemens was our first Executive Director. In that role he has streamlined and improved our processes (Knowlton's and Gift Store). Les's contributions to MICA are too many to capture here, but all should know that Les was instrumental in causing effective and positive changes to our professional corps association. Les has decided to pursue other activities. He will be missed. If you happen to see Les tell him thank you. We owe a great deal to this "Renaissance Man". Les's replacement is Mark Cline. Mark is the member's primary point-of-contact for MICA awards, membership, and membership issues. Mark brings a wealth of talent to MICA and he will carry on the tradition of excellence in support of our membership. You can reach Mark at [execdir@micorps.org](mailto:execdir@micorps.org).

Another new volunteer is John Dellagiustina. Many of you know John and of his limitless energy and talent. John has agreed to be our editor of *THE VANGUARD*. John has many ideas to improve *THE VANGUARD* and we look forward to seeing those changes in the near future.

It is scholarship season. MICA has scholarships to award to MICA members in good standing, their spouses and children. Our challenge is getting individuals to apply. SGM Koroll OCMI is our lead on this year's effort. He is doing an outstanding job getting the word out. We know there are deserving individuals who need assistance and we'd like to help. Scholarship information can be obtained by visiting our website: [MICORPS.org](http://MICORPS.org)

Lastly, we participated in the CSM Doug Russell ceremony honoring our Corps' most outstanding Non-Commissioned Officer. I was impressed by the significant contributions of Sergeant Julian M. Jones the CSM Doug Russell award winner. In reflection, no matter how difficult and challenging the problems presented to our Corps we should all take great comfort that we are blessed with the finest Soldiers in the world.

—Larry Bruns, President, MICA

## MICA National Executive Committee

### President

COL Larry D. Bruns, USA, Retired  
[president@micorps.org](mailto:president@micorps.org)

### Vice President

Mr. William F. Morgan, Jr.  
[vicepresident@micorps.org](mailto:vicepresident@micorps.org)

### Secretary

Mr. Christopher L. Friend  
[secretary@micorps.org](mailto:secretary@micorps.org)

### Treasurer

Mr. Rafael Monge, Jr.  
[treasurer@micorps.org](mailto:treasurer@micorps.org)

### For information on memberships, chapters and awards, please contact:

#### Executive Director

INCOMING: Mark Cline  
[execdir@micorps.org](mailto:execdir@micorps.org)  
OUTBOUND: Les Siemens

### For information scholarships, please contact:

#### Scholarship Program Coordinator

SGM Steven Koroll, USA

## Contents

MICA Scholarships	ii
Check your mailing label	ii
Notes from the President	1
Warfare Beyond Bounds	2
96B Training	5
Intelligence Collection	7
Integrating Social Sciences and Intelligence	11
Regression in Analysis	14
Deterrence and Terrorism.	15
Intelligence "Reach Back" Only Works if We "Reach Forward"	20
Integration of Psychology into Intelligence Production	22
MICA News	24
Northrop Grumman makes scholarship donation	24
Chapter News	24
31D leaders visit MI Group, speak at local MICA luncheon—Fort Gordon	24

---

# Warfare Beyond Bounds

---

## Strategic Intelligence Paper

by SFC Errol B. van Ommeren

ANCOC Writer of the Cycle

### Executive Summary

Will China engage in an Asymmetric War with the United States? The relationship between China and the United States has slipped substantially in recent years, to the point where a war may be a continuation of politics due to failed diplomacy. One question is if China chooses war with the United States, what will be the nature of the conflict? An answer may come from the book *Unrestricted Warfare*. Written by two Senior Colonels from the People's Liberation Army, *Unrestricted Warfare* proposes using Information as a weapon to deal crushing defeats without bloodshed. These new weapons include using International Law to erode a nation's Center of Gravity; Economics to disrupt a nation's cash flow, increase inflation and cause a breakdown of social order; Network Warfare to conduct espionage and block information flows; to Terrorism to create uncertainty. While these ideas are not new, *Unrestricted Warfare* describes them as new way for a nation to combat another nation with superior Command, Control, Communications, Computers and Intelligence. In reality, China is more than capable of conducting these attacks, is poised to devastate in some areas, and may already be conducting others. The United States should prepare for the full spectrum of these new weapons.

Will China engage the United States in an Asymmetric War? Late on Friday night, 7 May 1999, NATO warplanes accidentally bombed the Chinese Embassy in Belgrade, Yugoslavia.<sup>1</sup> Although both NATO officials and President William Clinton apologized to the government of the People's Republic of China for the accidental attack, press reporting internal to China and throughout the free world labeled the attack as intentional. After all, with the advanced Command, Control, Communications, Computers and Intelligence (C4I) supporting us, such a mistake should not be possible. Accusations and counter-accusations flew, conspiracy theories were spun, but in the end, the results were the same. The attack killed three Chinese Embassy workers; numerous others injured, further straining the diplomatic relationship between the United States and the People's Republic of China. The damage caused to the Chinese Embassy just may have been the opening salvo in an Asymmetric War between the United States and the People's Republic of China. Open for debate is the question of whether this historic low point in relations

between the United States and China was the start of another, more subtle conflict. With unresolved issues continuing to strain relations, from Tibet and human rights violations on one side, to support for Taiwan and spreading imperialism on the other, the question could be what will be the breaking point between these two powerful nations that will lead us to war.

Has that breaking point already arrived? Clausewitz stated, "War is a continuation of politics by other means". At the risk of sounding pretentious, this oft-quoted line may have more bearing than the United States may think. Could we be at war, a war with limited aims, against an enemy that chooses to wage war on a level that does not involve bombs and bullets? To draw that concept out further, is such a thing even possible? Have we reached a point in the Information Age where ideas are weapons, and terror, economics, laws and the media are the bullets that kill? If we look around us, the cursory evidence is unsettling. We have been engaged in a War on Terror that has stretched into its seventh year, with no end in sight. Millions of Americans are struggling with their finances, trying to pay their mortgages while the stock exchange drops. The United States finds itself unable to pass resolutions in the United Nations Security Council despite being a standing member of the Security Council. The media at large has set its sights on the United States, with pictures of mistreated prisoners and dead civilians from the War on Terror circulated around the globe. Against this backdrop, China finds itself in an advantageous position on the world stage. Having recently hosted the Olympics in Beijing and sent their first astronauts into space, China is looking and acting like a world leader. It may be that all of these events were manipulated, setting the scene for a greater conflict. China may be waging a new kind of war, based on new rules that the United States is learning all too slowly. At risk is the possibility of the international balance of power shifting east to China, with economic status, political influence and the standing of world leader hanging in the balance.

Through an examination of four points; Legal Warfare, Economic Warfare, Network Warfare and Terrorism, I will seek to answer the question on if the Chinese will engage in a "hot" Asymmetric War with the United States. The starting point, however, must take us as Americans away from our definitions of these kinds of warfare, as well as our very definition of war. To help us, we need to see the situation through our adversaries' eyes. In February 1999, two Senior Colonels from the People's Liberation Army (PLA) named Qiao Liang and Wang Xiangsui wrote the book, *Unrestricted Warfare* through the PLA Literature and Arts Publishing House in Beijing. The very fact that it was published is significant in itself. In a country with no freedom of

the press as we know it in the United States, producing literature that deviates from accepted party lines would be impossible, with the authors suppressed with draconian. *Unrestricted Warfare* lays out new ideas on what is a weapon, what is war, and how a nation prosecutes war in the future. Simply put, this is a manual on how to fight against an opponent that has the technological advantage on the battlefield. With nations unable to compete against the technological might of the United States, any future potential adversaries will look past their obsolete arsenals into our soft, Information Age underbelly. The authors of *Unrestricted Warfare* state, "As we see it, a single man-made stock-market crash, a single computer virus invasion, or a single rumor or scandal that results in a fluctuation in the enemy country's exchange rates or exposes the leaders of an enemy country on the Internet, all can be included in the ranks of new-concept weapons."<sup>2</sup>

International Law Warfare, or as coined by John Carlson and Neville Yeomans<sup>3</sup> and expanded on by Colonel Charles Dunlap in his paper, *Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts*,<sup>4</sup> "Lawfare," consists of using international law, international public opinion, and perceived societal norms to gain a military advantage. Very few Soldiers have not seen the effects. Through the permanent addition of Judge Advocate General Lawyers to Targeting Cells to detailed Rules of Engagement (ROE), Lawfare is here to stay. The concept is simple. If a nation is perceived to be fighting an unjust war by failing to adhere to International Law, Geneva Conventions, General Orders or the Rules of Engagement, popular support at home with the public at large will wane. This erosion of a nation's "center of gravity", the popular support from one's own population, could lead to the ending of the war on unfavorable terms. A domestic example is our own Vietnam War, with the Mi Lai Massacre forming one of the stepping-stones to an unsatisfactory conclusion. While clearly the Chinese government is not the puppet master behind the scenes, pulling the strings behind every Lawfare fumble we have committed on the battlefield to date, it is equally clear that they will reap the benefits. Xinhua News Agency, one of the major media outlets in China, reports directly to China's Communist Party. The international press will report every legal misstep. The added, albeit necessary, bureaucratic layer created by the addition of legal warriors slows down the Military Decision Making Process. Soldiers that are in doubt of their understanding of the ROE now questioning every action they take, or are about to take, with the specter of the Uniform Code of Military Justice hanging over them. China, through abstaining from getting involved in worldwide military action, has achieved something of a minor moral victory in the court of public opin-

ion. China has fumbled the Lawfare ball themselves. The international public has not forgotten about Tibet, Tiananmen Square, and the treatment of members of Falungong. The major difference is that China, whose government control of the media controls their public's opinion, has much less to lose.

Economic Warfare is a very central tenet of *Unrestricted Warfare*. Examples range from using banking to place a strangle hold on the finances of terrorist organizations to using proxies to manipulate international markets. The ultimate intent of a financial attack is to cause a collapse of social and political order. China has made inroads into U.S. business, but the attempts are comparatively small and exceedingly difficult to conduct in the face of legal constraints. United States law can be used to prevent or slow foreign investment. The Byrd Amendment to Exon-Florio<sup>5</sup> forces a mandatory investigation when any foreign nation conducts business in the United States that could affect national security. Comparing China to the rest of the United States' top ten trading partners, some key facts emerge that are causal to the use of the Byrd Amendment. One, China alone is not a strategic or political ally of the United States. Two, China alone maintains state ownership and control of companies. Three, major political and security issues remain between China and the United States.<sup>6</sup> With these conditions, China can be legally stopped from any business deemed a national security threat. On the other side of the coin, there is very little to prevent foreign banks from purchasing U.S. debt. As of July 2008, the PRC held 518.7 billion dollars in U.S. debt, second only to Japan. The United States has placed itself in a risky position. While unlikely, if China chooses to unload U.S. debt, it will cause a concerning increase in inflation.<sup>7</sup> In the global marketplace, China would not walk away unscathed. The difference is that a country with state control of business, the government can artificially prop up businesses during an economic crisis without the need for public consent. The economic pain suffered by the Chinese people would not be anywhere near the kind that the American people would have to endure. Considering the current state of Foreign Capital Investment, China stands poised to strike a devastating blow to the United States economy.

Network Warfare is consistent with current Chinese Asymmetric Military thinking<sup>8</sup>. Cyber attacks emanate daily from the PRC; the only question is who the guiding hand is? The surface evidence seems to point to the PLA. Aside from its analysis in *Unrestricted Warfare*, it seems that in a country with so many restrictions concerning information, only the government would be able to provide the resources needed to mount these kinds of attacks. From 2003 to 2005, a systematic series of attacks against U.S. Department of Defense (DoD)

networks dubbed “Titan Rain” broke into hundreds of computers.<sup>9</sup> Released information is clear on where the attacks originated, but again, the identity of the man behind the curtain is unclear. The United States is not the only victim. Aside from the numerous attacks mounted against the DoD and other U.S. Government agencies, Chinese hackers have attacked Germany and the United Kingdom.<sup>10</sup> Hackers conduct attacks for a variety of reasons, such as espionage, information gathering, denial-of-service, vandalism and propaganda. The authors of *Unrestricted Warfare* take this very seriously, stating, “Before very long, a network war ... might become a reality right in our midst, a type of war that nobody even imagined in the past. It is likely to be very intense, but with practically no bloodshed. Nevertheless, it is likely to determine who is the victor and who the vanquished in an overall war.”<sup>11</sup>

Terrorism is the bane of the existence of every nation on earth. Very little today is not tainted by it. China does not appear to sponsor terrorism, and in fact suffers from an internal terrorism issue from a Muslim minority. The examples from *Unrestricted Warfare* point to Osama bin Laden as a prime example of terrorism today. Where does China fit in the Asymmetric Warfare puzzle when it comes to terrorism? A country does not need to sponsor terrorism to reap the benefits from it. On the surface, China is cooperating with the War on Terror by providing information about its own domestic terrorism issues. Since China does not have the worldwide military footprint that the United States does, it need offer little more. While far from responsible for the type of terrorism we are facing today, “The only thing necessary for the triumph of evil is for good men to do nothing.” This acting by failing to act is consistent with one of the earliest writings on military strategy, Sun Tzu’s *The Art of War*. As the United States learns the enemy in Iraq and Afghanistan, China also learns about the United States. “Rouse him, and learn the principle of his activity or inactivity. Force him to reveal himself, so as to find out his vulnerable spots...Carefully compare the opposing army with your own, so that you may know where strength is superabundant and where it is deficient.”<sup>12</sup>

More frightening is the idea that these attacks will be used in combination with each other, and with other types of attacks. The only limit is the imagination. China is more than capable of conducting Asymmetric War with the United States, and at least on the level of Cyber Warfare, may very well be conducting Asymmetric Warfare right now. As it stands, it is quite clear that the Chinese are willing to use these new techniques, and are poised to exercise these new weapons. China recognizes the significant advantages the United States maintains in C4I. China has chosen a path to negate that advantage and replace it with techniques to deliver a crushing,

yet bloodless, defeat. The United States acknowledges some of these new tactics, but delineates some, such as economics, under politics. While still a form of National Power, failing to use that tactic at the same level of Information Age savagery against an opponent may be akin to taking a knife to a gunfight. In today’s age of Capabilities Based Warfare, the United States needs to perceive what other nations perceive as warfare, and develop Tactics, Techniques and Procedures to defeat the new capabilities. The authors of *Unrestricted Warfare* sum it up best, by saying, “If that young lad setting out with his orders should ask today: “Where is the battlefield?” The answer would be: “Everywhere.”<sup>13</sup>

## Endnotes

1. “NATO expresses regret, resolve after bombing Chinese embassy,” CNN, 8 May 1999. Retrieved 25 October 2008 from <http://www.cnn.com/WORLD/europe/9905/08/kosovo.03/>
2. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), 25.
3. John Carlson and Neville Yeomans, “Whither Goeth the Law - Humanity or Barbarity,” *The Way Out - Radical Alternatives in Australia*, ed. M. Smith and D. Crossley (Melbourne: Lansdowne Press, 1975).
4. Colonel Charles J. Dunlap Jr., *Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts*, (Washington, DC: Carr Center for Human Rights Policy Kennedy School of Government, Harvard University, 2001), 1.
5. Edward M. Graham and David M. Marchick, *U.S. National Security and Foreign Direct Investment*, (Washington, DC: The Peterson Institute for International Economics, 2006). 104.
6. Graham and Marchick, 104.
7. Steve Whitehouse, “BIS says global downturn could be ‘deeper and more protracted’ than expected,” *Forbes*, 30 June 2008, para. 21. Retrieved 26 October 2008 from <http://www.forbes.com/afxnews/limited/feeds/afx/2008/06/30/afx5166493.html>
8. Annual Report to Congress, *Military Power of the People’s Republic of China 2008*, (Washington DC: Office of the Secretary of Defense, 2008), 3.
9. Dawn S. Onley and Patience Wait, “Red Storm Rising,” *Government Computer News*, 21 August 2007, 2. Retrieved 26 October 2008 from [http://www.gcn.com/print/25\\_25/41716-1.html?page=2](http://www.gcn.com/print/25_25/41716-1.html?page=2)
10. Annual Report to Congress, 4.
11. Qiao Liang and Wang Xiangsui, 43.
12. Sun Tzu, *The Art of War*, Chap 6 para. 23-24. Retrieved 26 October 2008 from <http://stockmarketbooks.blogspot.com/2008/06/art-of-war-chapter-6-weak-points-and.html>
13. Qiao Liang and Wang Xiangsui, 43.



---

## 96B Training

---

by Roger Howard, MSG(R), USAR

Recently, I read Mr. Adam's article on 35F training in the Fall 2005 issue of *THE VANGUARD* and also Mr. Hammer's response in the Winter 2006 Vanguard. Both individuals have done a superb job of critiquing OB training and laying out suggested improvements. As a former 96B I can not resist commenting.

First, Ft. Huachuca does a good job of taking a young soldier just out of high school and training him to become analyst. I would not want the job. It is difficult because a 35F has to be a subject matter expert (SME) in multiple areas: military ops, both Blue and Red, the S2 shop which includes personnel and physical security, data security, enemy order of battle, weapons, SITMAP, and others. Considering the task of training a young soldier with no military and very little life experience, Ft. Huachuca does a fine job and the staff is dedicated and hard-working.

We all agree that the training needs to be improved. But how? What is a 35F and what should the soldier know? Extending AIT from four months to six or eight months will not improve the training if we can not define an intelligence analyst. The 35F job I held in the DISCOM S2, 8th ID(M) was completely different from my intel job in OPDET 1, 8th PSYOPS Bn. Looking back I realize both positions had their favorable points. The PSYOPS job taught me basic strategic intel, which included tribal studies, politics, economics and geography, plus some specialized topics like television and radio broadcast systems, rail gauges, road construction and electrical power generation.

The DISCOM S2 job concentrated more on S2 ops rather than intelligence. Personnel and physical security were almost full time positions, and added to those responsibilities were map and document custodian and emergency action duties. Daily the staff duty officer and NCO reported to the S2 for current situation briefings and under certain threat levels the Rose Barracks (Bad Krueznach, Ger.) guard force fell under the DISCOM S2. Possibly the most important lesson I learned from this job was how the different staff sections worked and interacted with each other. Interpersonal skills was just as important as any FM.

My wife was assigned to the division ASPS. Her position was more of the traditional Cold War OB analyst. She tracked Warsaw Pact and GSFG forces. The number and type of tanks were significant as were the artillery and NBC forces. From memory I think I can still plot those Soviet forces coming through the Fulda Gap.

Those slots were three TO&E OB positions and yet all

three were completely different. If we are to effectively train intelligence analysts, we need to decide what an analyst should know and do. The alternative is to accept that all 35Fs need a rudimentary level of intel training and the specific tasks will be assignment driven. Those intel slots at the maneuver battalions will be security oriented with increasing intelligence focus beginning with the brigades. In effect, most of the training beyond the rudimentary level will be gained through OJT.

If we accept this alternative outlook, the unit MI training becomes much more important. I was fortunate because the 8th PSYOPS Bn CSM drove intel training. His emphasis on tactical MI/PSYOPS forced the lower enlisted to learn the operations. Unfortunately, the emphasis on unit training throughout the army is inconsistent. The result is poorly developed intel NCO's. I met many 35F E5's and E6's who could not remember how to run a SITMAP because the last one they had completed was in AIT.

In order to make up for the lack of unit MI training and the disparate MI experiences of young analysts, BNCOC must become the course of intense intelligence training. We should increase the length, breadth and intensity of BNCOC and this course must become the bedrock of intelligence analysis. At the BNCOC level, the soldier has enough experience to understand how a complex organization, such as a maneuver brigade operates and the role the S2 shop plays. Until the soldier achieves this level of experience, the best training is too abstract to be used effectively by a young 'just out of high school' soldier.

As an NCO, I realize when I get an E2 from Ft. Huachuca, he knows very little about the army or intelligence. It is my job to teach him both. I also understand that E2's and E3's will spend a lot of time on 1SG details. I have to make the most of the limited times when I have that soldier but how much he learns depends on his level of motivation. There is very little time for formal training while on duty; if the soldier wants to learn the job, he must take advantage of every opportunity, online and correspondence courses, on post colleges and many others. Being an analyst is not easy and being a good analyst is not for the unmotivated.

The 35F MOS is the broadest and most poorly defined intel job in the army. These two characteristics make training difficult. Rather than focusing on adding more topics to AIT, I would shift the emphasis to BNCOC. A graduate of BNCOC must know how to run an S2 shop and be both fully capable strategically and tactically. The course would include many classes that most analysts never take. BNCOC should add portions of the security manager's course, elements of Battle Staff and the old S2 combat ops course and the old "Whiskey" PSYOPS

course that was taught by the JFK Institute for Military Assistance at Ft. Bragg.

The PSYOPS course consisted of basic cultural sociology, economics and several other topics that are relevant to the current ops in OEF/OIF. The security manager's course included physical security (changing lock combinations) and personnel security and other areas that relate to running an S2, albeit not strictly MI subjects. The Battle Staff and S2 combat ops courses concentrated on operating a tactical S2 with some insight into how the other staff sections functioned and related to intel ops.

The cost of running BNCOC in this way will be high. In order to allay some of the expense, Ft. Huachuca can outsource portions of or the entire course to the reserve MI battalions at the DIVITS (Division Institutional Training). These MI Bns are conveniently located throughout the U.S. They are located near Boston, MA, Ft. McCoy, WI, Ft. Huachuca, Camp Parks, CA, Camp Bullis, TX, and Ft. Bragg, NC. The 6th MI Bn, 3rd Bde, 108th Div. (IT) at Ft. Bragg, my old unit, ran classes throughout the Southeast: Orlando, FL, Jackson, MS, Ft. Bragg, Birmingham, AL, and Atlanta, GA. This capability is essential in reaching a geographically dispersed target market of reserve and guard soldiers and is applicable to the active component, as well. Using the DIVIT's unique capability to support a large geographic area will drastically reduce TDY and PCS costs. Additionally, soldiers attending BNCOC will not be separated from their families for additional extended periods. Classes can be completed one weekend per month for 8 or 9 months with a 2 to 3 week resident course at the respective MI Bn's home station.

The expectations of Ft. Huachuca producing fully functional intel analysts are unrealistic. It takes time to develop a soldier. Unfortunately, because of OIF/OEF there is not much time for developing young analysts. It is incumbent upon the NCO corps to make the effort to both train soldiers and to provide input into what needs to be taught at the school house. Without this input, Ft. Huachuca will be operating blindly and their product may not meet the needs of the end user.

I sound highly critical of new analysts. I am not denigrating the new 35F or downplaying his abilities or contributions. Units cannot function without them and most of the new intel soldiers I have met are highly motivated and very talented, much more so than I was at their age. I am impressed with the young MI soldiers because they are very bright, eager and readily adaptable.

The school at Ft. Huachuca, rather than attempting to train recruits 'to be all things to all people' should focus on a narrower intel perspective and train those tasks well instead of many tasks poorly. Instead of expanding AIT, we need to better define a 35F and align the training

with that definition. After defining the analyst's job, we will be better able to determine what an AIT graduate's needs are. From this determination we can tailor unit training that will further develop the soldier.

Ft. Huachuca must fully use the ARISC's (Army Reserve Intelligence Support Center) and the DIVIT MI Bns to support MI training. Both the ARISCs and the MI Bns can provide high quality and specific exportable training packets across the U.S. Instead of sending everyone to Ft. Huachuca, the ARISCs and MI Bns can run the classes at the requesting unit's installations. Also any newly developed courses can be field tested in multiple locations and the feedback can be sent directly to Ft. Huachuca.

Being an intel analyst was a challenging job but also one of the most enjoyable. The scope of a 35F is broad and because of that I was able to get my fingers into many different aspects of intelligence. But until I gained this experience I was not as productive as I should have been.

Taking years to develop an MI soldier like I was is wasteful. Instead of debating the merits of expanding AIT and the benefits of training the old Soviet model versus asymmetric warfare, we need to more fully define a 35F. Second, we need to fully use the MI training assets available and take advantage of the capabilities of those units to provide tailored and transportable MI instruction.

I said it earlier but I will say it again. Ft. Huachuca does a good job of training the 'fresh off the block' soldier.

Always out front.



*Ed Note: MSG(R) Howard has agreed to publish his email for reader comments: howslide@yahoo.com.*

*His service biography includes 24 years active & reserve Army (MOS's 96B & 37F). He has worked as Chief Instructor and course manager, teaching the 10 course and BNCOC and ANCOC. Mr. Howard concludes that his 35F intelligence training ranges "from grease pencils and acetate to computers."*

---

# Intelligence Collection

---

by Angela Brown

The global community is threatened with a faceless and borderless enemy that must be confronted by a unified effort. International relationships between political states will require increased information sharing to combat the terrorist threat. To have the most effective and actionable intelligence available to combat the common enemy, political entities will be forced to cooperate on the international level. Global terrorist networks operate and cooperate without constraints of borders or governmental obligations. To adapt to the terrorist threat, a social contract and cooperative agreements in the global international community (GIC) will require tailored information sharing policies, the capability to act on the information, and regulations on its governance overseen by an independent body.

The September 11, 2001 attacks help argue the need for increased cooperation in information collection and analysis. The United States has undergone drastic reorganization and consolidation for efficiency and effectiveness. It was known that each intelligence or anti-crime organization within the US had its own functions and collected its own information by whatever means in which it specialized. The communication and coordination efficiencies between the major domestic and foreign focused US intelligence collection agencies “failed to connect the dots” of the pending terrorist attack because they did not communicate (Diamond and Kiely 2002).

Since September 11, the US intelligence community (IC) has established the Department of Homeland Security, National Counterterrorism Center (NCTC), and the Director of National Intelligence (DNI) position who oversees the IC. One of the required changes involved converting the IC community director into an unbiased overseeing position in the government who answers directly to the President. Previously, the IC director position was also the Central Intelligence Agency director, called the Director of Central Intelligence (DCI). The effort to remove any biases, establish deconfliction and a central point for intelligence direction, was an important step for the progress and improvement of the IC coordination and functionality (Best 2005). As a whole, the international community will need to have the similar ability to adapt and consolidate leadership focus to combat the threat.

Throughout US history there have been changes required in the US intelligence community because of significant events. One example in progression of national intelligence coordination as a result of failed

policy was the 5412 Group. The use of covert action and the resulting political problems led to the creation of working groups, task forces, or congressional intelligence oversight committees. The 5412 Group was established when the original group created to mitigate policy issues was not effective. Planning Coordination Group was not “senior” enough and did not have the “need to know” for Authority and direction on Covert actions (Prados 1996, 112). The correction led to the 5412 group which consisted of senior officials who were direct designees of the President, State Department, and the Pentagon. The DCI was also a member of this committee which was under the direction of the National Security Council (NSC). Since its founding and numerous reorganizations, it developed into the National Security Planning Group consisting of the heads of each major intelligence organization under President Reagan and is now a decision making body within the NSC (Whitehouse Press).

Consolidation, coordination, and decision making concerning intelligence activities have adapted as required through history. The national decision group continued to evolve and encompass all security aspects leading to the decision making body to be created within the NSC (Whitehouse Press). Though these organizational changes, the intelligence collection methods have progressed naturally or with the incorporation of technological advancements. In its current organization, members representing each of the major security agencies and other organizations, assist the president in foreign and domestic policy development. Because the council concerns one country, it can have policies and actions carried out by the respective part of government for which it applies. The need for similar cooperation and coordination on a global level is increasingly apparent.

Parallel or similar changes will need to take place on the international level so that the maximum effectiveness of information collected is integrated and used effectively to confront the global threat. An understanding of the requirements to combat new threats will enable the global community to take advantage of the adaptations that the US had to make to maintain effectiveness. Classical social contract theories hold that to move away from the state of nature (chaos), individuals (political states) will enter a social contract to secure their respective interests.

According to the Grotian theory, an international society’s ability to function is based on “the acceptance of the requirements of coexistence and cooperation in a society of states”, not the “illusion” that transnational loyalties from an established society will not outweigh the realities of war between those states (Bull 2006, 38-39). The necessity for a common information shar-

ing entity will not dismiss the realities of potential wars between states. It will, however, eventually lead to the establishment of an independent supranational body that will not rely on political status between states to affect its anti-terrorism functionality.

By applying the principles of the Social Contract theories and adapting those principles according to necessity, the international community will require organization and cooperation to fight terrorism. To note what is needed for integration, the current institutions in place need to be examined. Current international cooperative organizations that provide some semblance of information sharing and collection include the European Union (EU), the North Atlantic Treaty Organization (NATO), and the United Nations (UN). Even with these collective bodies, there is still not an over arching global information collective entity that benefits all states and has the ability to extinguish the threat.

The EU recognizes the necessity of a common effort. According to a council decision proposal sent before the Commission of the European Communities in 2005, the "transmission of all relevant information [...] to Europol" that is "resulting from the activities of national security and intelligence services" is to be shared with other member states for the prevention and combating of terrorism (COM(2005) 695 Final). This mandated relationship from security vulnerabilities is the way ahead for the GIC and lessons can be applied to a similar working relationship with other organizations. A major advantage that the EU has over other organizations is the common cultural values between states. The similar languages, the familiar culture and proximity, as well as the common economic interests of the states involved, has afforded less animosity among them and allowed the establishment of a social contract for the common good.

NATO was formed to benefit mutually its member states and ensure the collective security by political and military means (Yost 2001). NATO has a military capability and has employed it in various parts of the world. Although a collective security establishment,

[...] many of the essential activities of the fight against terrorism occur outside NATO, through bilateral cooperation or loose coalitions of the willing. Three factors help to explain NATO's minor role in combating terrorism: shifts in alignments and threat perceptions caused by systemic changes, the alliance's limited military capabilities, and the nature of the fight against terror itself. Over time the consequences of NATO's limited role could be severe. If NATO's strongest members do not seek to address their core security threats within the alliance, NATO may have difficulty sustaining its military value (de Nevers 2007).

NATO does not maintain a global area of respon-

sibility and is only accountable to North America and Europe. Furthermore it is common with the EU in that democratic and cultural similarities contribute to cooperation and mutual interests. Additionally, to become a member of NATO, sovereignty is not jeopardized and each state contributes equally. Because of the cold war mindset at the time of its establishment, NATO countries have developed a system to contribute intelligence to the common good (NATO 2001). This mutually beneficial type of social contract was easy to enter as the political ideals of democracy and collective security are the common culture against the common enemy of non-NATO states.

Although NATO shares information as a group, bilateral relationships are sometimes stronger between some NATO members than others. These relationships allow for the information that is shared to be sometimes more sensitive in nature. Bilateral relationships are also effective at improving certain political and economic ties but do not contribute to the group as a whole. A bilateral relationship encourages exclusion of cooperative information sharing relationships with other states. To enter into a social contract for true collective security, a true and globally reaching collective security entity would require some amount of sacrifice in political ideologies in exchange for the search of a common culture necessity to combat a common enemy. Unlike the EU, NATO has the added benefit of a military alliance; however, the US has refused to allow any other nations command or control of its forces. As described by Yost;

More ambitious aspirations, for a collective security system in the Kantian or Wilsonian sense, would compete with a collective defense orientation, because these aspirations call for replacing balance-of-power arrangements and alliances, which are by definition exclusive, with an inclusive community in which peace and security would be truly 'indivisible' (Yost 2001).

A close relationship with all members, not just bilaterally, is required for complete security. The problem with classical social contract theoretical thought is that the terrorist organization is not recognized as an entity and therefore would not obligate its self into a social contract for the collective security. Inherent in the nature of western political ideals, military power is what determines the success of a political state. The rise of asymmetrical warfare without moral or political obligation disregards the need to join a social contract for military unity. It does obligate all other political states to form a cooperative effort against the outsider threat.

Throughout its history the US has recognized the importance of military coalition building. More recently with the coalition forces in Iraq and Afghanistan,

the intelligence sharing is critical to battlefield success (Washington Times 2007). The US has allowed the close information and asset sharing relationship because the security benefits outweigh the cost. The US involvement in the international community is bitter-sweet. For legitimization, the US must be involved but often refuses fully to comply as;

[c]urrent U.S. treaty behavior is anachronistic in an era of globalization and interdependence. It denies Americans the international support required to resolve critical global and regional problems. The United States has long been ambivalent in its attitude toward international agreements; both leader and laggard. It exhorts others to change their behavior in international law but hedges American acquiescence with delays and conditions. Today this attitude has hardened into near contempt for the law of nations. [...]. Not only do Western democracies limit their participation by the same methods, but countries governed by Sharia law also carve a wide swath of exemptions from the human rights treaties they sign. Other signatories tolerate these deviations both in the interest of universality and, in the case of America, because of the symbolic or actual importance of its inclusion in an international regime (Chayes 2008).

The US is largely self-reliant when gathering information but still requires the assistance of international partners. For the international body to be effective, the US must agree to contribute information and allow some compromise of sovereignty concerning anti terrorism operations.

Again, NATO members are regionally and culturally similar allowing for the development of the current information sharing relationship. The GIC has yet to face a single threat to the unified community. Because of this reason, the GIC has not established a single entity above all others for the coordination and sharing of anti-terrorism intelligence. Only a supranational entity with the authority and legitimacy of the UN would be sufficient to combat the common threat.

The UN will not be allowed to completely be governed by democratic or western principles because of the vast differences of nations that would be involved in this social contract; the common culture must be security. The UN has the most number of state members of any cooperative entity. It has established the greatest credibility and would make the most effective and legitimate authority for the information sharing entity. The UN currently cooperates with Interpol on criminal matters. Unlike the EU's relationship with Europol, the UN-Interpol relationship does not mandate that information is sent in by member states. Furthermore, Interpol is

strictly used for the cooperation of international criminal matters and cannot be employed for military, political, racial, or religious intervention or activities (Interpol 2008). Although the Interpol-UN relationship has promise, at its current state, it is ineffective in fully collecting and executing actionable intelligence to prevent terrorist threats as a collective effort.

An ideal information sharing entity would be very similar in structure of the Interpol. Interpol has seven regional offices and maintains a centrally located main command body. Its regional offices function as consolidation points and are the points of contact between the command and the local law enforcement. Each member state contributes an annual amount to the budget. They maintain many databases for criminal investigations and unlike with intelligence sharing, are able to share freely the information with others without hesitation. The leadership rotates and many nationalities are employed at Interpol. The leadership is a 13 member regionally based General Assembly, where decisions are overseen and the day-to-day activities are the responsibility of the Secretary General (Interpol 2008). Each country representative has equal weight in the assembly and therefore potential biases are limited. It is understood that sensitive crime information is received and channeled into the main body for international criminal investigations. Interpol and the UN liaise effectively and often as required.

An international organization with mutually cooperative working relationships is what is needed to combat terrorism. Law enforcement is somewhat easier to negotiate than the sharing of sensitive intelligence between states. Law enforcement agencies also have the advantage of established jurisdiction relationships. Interpol is able to use the established criminal fighting entities that are local, who are the subject matter experts of their areas, to perform missions. The ongoing development of US-EU cooperation against terrorist efforts is still facing judicial and jurisdiction issues (Archick 2006). Intelligence cooperation and coordination relationships are much more difficult to establish and lack the operational arm to take advantage of the actionable intelligence.

Using the successes and failures experienced in other former or current intelligence sharing entities, a competent and efficient, unbiased organization, must be established that includes certain criteria on how to handle intelligence. This criterion includes methods and capabilities protection, and a common reporting and classification system. The organization will require restrictions and policy guidance that will protect each member country's collection methods. Inevitably, methods and procedures will be exchanged for greater efficiency.

To prevent the unnecessary compromise of capabilities or sources, a type of summary reporting would need to be established. Similar to the CIA summary of information sent to the NCTC, a common format should be used that provides the critical and time sensitive intelligence to the decision makers. A supranational entity with no particular state ties will provide the needed independent and non biased analysis. The analysts involved should be fully trained for a joint environment and be fully vetted by the international body. Above all else, intelligence sharing requires trust built on a mutually beneficial goal or outcome. The incentives include the access to previously unavailable information about a country or a region not accessible by states organic capabilities. Ultimately, the compromises involved with sharing information lead to the gains of the desired mutually beneficially relationship.

Although the desired collective security is what will be the overwhelming factor for participation, states may still hesitate for various reasons. Economic issues of who will pay for operations, political relationships between enemies, security mistrust of the information being mis-used or stolen, or fears of neocolonialism by western powers may prevent a successful information sharing relationship.

Similar to that of the US domestic agencies, as the number of international intelligence groups established increases, so will the increase for cooperation and coordination be required by a de-conflicting and directing independent entity. Lastly, the organization will need the capability to take action on the information when necessary. Neither Interpol nor the UN has the ability within their respective charters to execute military actions when necessary. The UN is primarily focused on Peacekeeping operations. To be an effective counter-terrorism entity, today's international society must also project that it has an effective arm of action. Also, political culture must be considered. Many western ideals hold that the possession of military powers is important to a state's international status. However, these western bodies prefer to employ diplomacy as a method of conflict resolution. This mindset does not hold true to many other member state cultures. The UN authorized body for action on intelligence information will require the hard power capabilities of an elite para-military nature.

Due to the increasing threat of a globally networked enemy, the international community will be forced to establish a global intelligence entity that directs all other regionally joined, or otherwise formed, intelligence cooperatives. Regardless of the entity that is established, increased cooperation on a global scale is required to counter the growing threat. A fruitful relationship will allow the needed coordination, adaptability, and flexibility

to counter and pre-empt terrorist network advantages on the current global state of intelligence cooperation. A future intelligence sharing entity operating within certain restrictions on collection elements and specific intelligence sharing policies agreed on by all parties involved will afford increased effectiveness against the growing international threat.

## References

- Archick, Kristin. 2006. U.S.-EU Cooperation Against Terrorism. CRS Report for Congress. <http://www.fas.org/sgp/crs/terror/RS22030.pdf> [accessed October 16, 2008].
- Best, Richard A. The Director of National Intelligence and Intelligence Analysis. CRS Report for Congress. [http://www.terrorsiminfo.mipt.org/pdf/CRS\\_RS21948.pdf](http://www.terrorsiminfo.mipt.org/pdf/CRS_RS21948.pdf) [accessed October 16, 2008].
- Bull, Hedley. 2006. The Idea of International Society. In *Classic Readings and Contemporary Debates in International Relations 3rd ed.*, ed. Williams, Phil, Donald M. Goldstein, and Jay M. Shafritz, 36-39. Belmont, CA: Thompson Wadsworth.
- Chayes, Antonia. 2008. How American Treaty Behavior Threatens National Security. *International Security*, (Summer): 45. In the Lexisnexis Database, <http://www.lexisnexis.com.ezproxy.apus.edu> [accessed January 2, 2009].
- Commission of the European Communities. December 22, 2005. Proposal for a Council Decision on the Transmission of Information Resulting From the Activities of Security and Intelligence Services with Respect to Terrorist Offenses. COM(2005) 695 Final, 2005/0271 (CNS), Brussels. [Http://eur-lex.europa.eu/LexUriServe/site/en/com/2005/com2005\\_0695\\_en01.pdf](http://eur-lex.europa.eu/LexUriServe/site/en/com/2005/com2005_0695_en01.pdf) [accessed October 16, 2008].
- Diamond, John and Kathy Kiely. 2002. Administration, Agencies Failed to Connect the Dots. May 17. *USA Today*. <http://www.usatoday.com/news/washington/2002/05/17/failure-usatcov.htm> [accessed January 2, 2009].
- Ford, Harold. Ed. 1997. Why CIA Analysts Were So Doubtful About Vietnam: Unpopular Pessimism. <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/vietnam.html> [accessed October 19, 2008]
- Gomper, David C. 1998. National Security in the Information Age. *Naval War College Review*, v. LI, no. 4, (Autumn): 22-41.
- International Police. Interpol: an Overview. <http://www.interpol.int/Public/ICPO/FactSheets/GI01.pdf> [accessed January 2, 2009].
- Issacson, Jeffery and Kevin O'Connell. 2002. Beyond Sharing Intelligence, We Must Generate Knowledge. *Rand Review* 26, no. 2 (Summer): 48-49. <http://www.rand.org/publications/randreview/issues/rr.08.02/intelligence.html> [accessed October 16, 2008].
- Lahneman, William J. 2004. Knowledge-Sharing in the Intelligence Community After 9/11. *International Journal of Intelligence and CounterIntelligence*, 17 no. 4:614-633. [http://pdfserve.informaworld.com/885808\\_793127654\\_714035498.pdf](http://pdfserve.informaworld.com/885808_793127654_714035498.pdf) [accessed January 2, 2009].
- de Nevers, Renée. 2007. NATO's International Security Role in the Terrorist Era.

International Security 31, no. 4 (Spring):34-66. In the Lexisnexis Database, <http://www.lexisnexis.com.ezproxy.apus.edu> [accessed January 02, 2009].

NATO. 2008. Improving Intelligence Oversight in Ukraine. NATO News. 4 April. <http://www.nato.int/docu/update/2008/04-april/e0421a.html> [accessed October 19, 2008].

NATO. 2001. NATO Open source Intelligence Handbook. [http://www.oss.net/dynamaster/file\\_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf](http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf) [accessed October 19, 2008].

NATO. 2001. Military Organisation and Structure; Chapter 11. <http://www.nato.int/docu/handbook/2001/hb1103.htm> [accessed October 19, 2008].

Prados, John. 1996. Presidents' Secret Wars. Elephant Paperbacks; Chicago.

Schreier, Fred R. Combating Terrorism and Its Implications for Intelligence. In CIAO Database, <http://www.ciaonet.org.ezproxy.apus.edu/wps/wit02/wit02k.pdf> [accessed October 16, 2008].

United Nations. UN Human Rights Chapter. Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Chapter VII, Article 39. <http://www.unhcr.ch/html/menu3/b/ch-chp7.htm> [accessed 2 January, 2009].

United States Whitehouse. History of the National Security Council. <http://www.whitehouse.gov/nsc/history.html> [accessed January 2, 2009].

Washington Times. 2007. Pentagon raises bar of intelligence-sharing. September 28. The Washington Times, national edition. <http://www.washintontimes.com/news/2007/sep/28/pentagon-raises-bar-of-intelligence-sharing/> [accessed October 16, 2008].

Yost, David S. 2001. NATO's Contributions to Conflict Management. In *Turbulent Peace: The Challenges of Managing International Conflict*. Ed. Crocker, Chester A. and Fen Osler Hampson and Pamela Aall. United States Institute of Peace Press, Washington D.C.



Angela Brown is a student at American Military University (AMU) completing a master's degree in Strategic Intelligence with an Operations concentration. Ms. Brown is a Military Intelligence branched 1LT in the Georgia Army National Guard and was previously enlisted as a CI Agent with the 221st MI BN. She is currently employed full time for the Department of the Army.

---

## Integrating Social Sciences and Intelligence

---

By 2LT Lindsey Champion

*VanDeman Program paper*

Army leaders recognize the importance of socio-cultural dynamics in Iraq and Afghanistan but are continually facing challenges on how to prepare soldiers for these dilemmas. In 2003, the Pentagon began the Human Terrain System project in hopes of meeting the military's local cultural and ethnographic intelligence needs. Understanding culture in Iraq and Afghanistan is instrumental for the military. With the proper understanding, the military is able to influence the population through non-lethal means by promoting stability, peace and economic and social development. The purpose of this paper is to highlight a solution to the Army's increasing need for accurate socio-cultural intelligence among junior officers and enlisted ranks by requiring anthropology and sociology training in basic courses.

According to then Major General Benjamin C. Freakley, "Cultural awareness will not necessarily always enable us to predict what the enemy and noncombatants will do, but it will help us better understand what motivates them...and how we can either elicit the support of the population or at least diminish their support and aid the enemy."<sup>1</sup> Current forces deployed in Iraq and Afghanistan often lack the cultural knowledge to maximize the effects of the military decision-making

process. In the counter-insurgency fight, it has become evident that the civil societies in Iraq and Afghanistan are the center of gravity. The civil society disrupts as unmet expectations emerge and feed a growing insurgency. The people often tolerate insurgencies because of their own dissatisfactions. This toleration often fuels an insurgency. Thus, it is imperative for the military to accurately understand these unmet expectations and frustrations of the civil societies in Iraq and Afghanistan. "It is imperative to view them from the perspective of the cultures in which the insurgencies are being waged."<sup>2</sup> LTG Peter Chiarelli, former Commanding General, Multi-National Corps-Iraq further detailed the cultural intelligence gap in Iraq stating, "I asked my Brigade Commanders what was the number one thing that they would have liked to have had more of, and they all said cultural knowledge."<sup>3</sup>

In order to meet this need, the Foreign Military Studies Office (FMSO), a U.S. Army Training and Doctrine command (TRADOC) organization established the Human Terrain System in order to "integrate and apply socio-cultural knowledge of the indigenous civilian population to military operations in support of the commander's objectives."<sup>4</sup> This program is meant to address cultural awareness shortcomings at the operational and tactical levels and introduced the concept of "human terrain." Human terrain is defined as the social, ethnographic, cultural, economic and political elements of the people among whom a force is operating by Montgomery McFate, one of the main architects of the Human Terrain Team.<sup>5</sup> The Human Terrain Team (HTT)

is the core building block of the Human Terrain System. The HTT includes five personnel (two military and three civilian) that are embedded in each forward-deployed brigade or regimental staff. The team will consist of the HTT leader, a cultural analyst, a regional studies analyst, a human terrain research manager and a human terrain analyst.

The HTT also can employ its reach back connectivity to a network of subject-matter experts (SME). In 2007, Secretary Gates authorized a forty million dollar expansion of the program. As of October 2007, the number of teams in Baghdad was expanded from one to six; thus, HTTs are eventually expected to be assigned to each of the 26 combat brigades in Iraq and Afghanistan.<sup>6</sup>

HTTs on the ground are currently contributing to military operations in both Iraq and Afghanistan. Since HTTs were first deployed, several officers have praised their ability to improve socio-cultural understanding. Colonel Martin Schweitzer, commander of the 82nd Airborne Division, noted that the unit's combat operations had reduced by sixty percent after the employment of the HTT.<sup>7</sup> However, HTTs are only at the brigade and regimental levels, which may leave battalions and lower with a disadvantage in the military decision making process. Additionally, the military personnel on HTTs are often majors and above. While HTTs provide key information to brigade commanders, focus should also be given to lower echelons. Each echelon in a brigade has its own respective area of operation (AO) which also has unique human terrain issues. A five person team may not necessarily have the capability to analyze the socio-cultural structures in an entire brigade AO as possible.<sup>8</sup>

HTTs are legally prohibited from collecting actionable intelligence. The HTTs do not collect intelligence or have a role in targeting. The role of the HTTs is to advise soldiers and leaders on how to interact with locals within the area of operations and to help them understand the population. The HTS is an open-source, non-classified program that uses social scientists. And, while HTTs have found some successes, in the United States, HTTs are still considered controversial. The American Anthropological Association has demonstrated disdain for HTTs stating that the Army program violates the AAA code of ethics. In order to meet these possible structural and ethical challenges, commanders should focus on training military intelligence personnel in anthropology and sociology. While anthropologists and social scientists are legally prohibited from collecting intelligence on the population, military intelligence personnel are not ethically prohibited from gaining a better cultural understanding. HTTs provide great cultural insight to brigades, but are placed in a position that may undermine their effectiveness because of homefront controversy, high

level dissemination and an inability to synthesize cultural awareness and intelligence to produce more timely information for military objectives.<sup>9</sup>

It is true that military intelligence officers and enlisted personnel especially need additional cultural awareness training for deployments to Iraq and Afghanistan. However, instead of focusing on specific cultures, the Military Intelligence Corps should focus on providing intelligence personnel the framework for how to understand cultures through anthropology and sociology training. This way, intelligence professionals will be able to adapt to the changing contemporary operational environment, analyze differences in sub-cultures within the area of operations, and begin to exploit the socio-cultural intelligence to enhance military objectives.

The first course of action I recommend is to require ROTC and West Point cadets three credit hours of Anthropology and/or Sociology for those entering the Military Intelligence Branch. Currently, ROTC and West Point cadets learn what their branch will be by at least the completion of their junior year in college. This allows for cadets interested in branching military intelligence to plan ahead by taking the required course and for those did not plan ahead, an additional year to take the course. A challenge to overcome in this course of action is that not all colleges have an anthropology or sociology course offered in the course catalog. Additionally, even if all the colleges have the courses they will not all be the same or taught with the same books/materials. One way to overcome that is to develop a curriculum for Anthropology or Sociology and add it to the ROTC program, as well as the core curriculum at West Point. An alternative approach to this course of action is to provide ROTC and West Point cadets incentives for majoring in a social science or taking social science courses.

A second course of action I recommend is to insert Anthropology/Sociology course into the Military Intelligence Basic Officer Leadership Course (MIBOLC). I recommend adding an additional four week long course centered entirely on social sciences and intelligence, and how to exploit cultural understanding in intelligence collection. A possible challenge for this course of action is that there is not enough time or funds to add an additional component to MIBOLC. If an additional phase is not feasible, I would recommend that anthropology or sociology theories be added to the Critical Thinking section and the Van Deman Program. Additionally, MIBOLC should consider recruiting former HTT leaders for guest lectures. A similar program can also be added to the Military Intelligence Advanced Individual Training (AIT), as well as the NCO Academy.

A third course of action I recommend is to require both military intelligence officers and enlisted

personnel to complete an online course for anthropology and sociology. This course would occur after basic training, once soldiers reach their units. S-2 shops or MI platoons could take the course simultaneously, which allows for officers in those units to facilitate the course and discussion on the importance of social sciences in intelligence. The course could occur in cycles as to facilitate the incoming and outgoing personnel. This course of action will be cost effective and will not require additional time away from units. The online program could be ran by a team of experts with a background in Human Intelligence at Fort Huachuca. A possible course of action in the future could entail creating a new MOS intended specifically for the purposes of anthropology or sociology and human intelligence.

These courses of action require funding, development and time in order to be effective. If none of these are feasible at this time, I recommend the HTTs should implement the following actions in order to aid military intelligence personnel's understanding of the battlefield: have briefings with military intelligence officers below brigade in order to familiarize them with anthropological and sociological intelligence, provide military intelligence personnel access to the reachback link which draws on government and academic sources to answer any cultural or ethnographic questions, and train military intelligence personnel on analyzing human terrain through HTT products.

Lastly, as military intelligence personnel continue to use Intelligence Preparation of the Battlefield (IPB) as a framework for military decision-making, focus should be added to Step 2: Describe the Battlefield Effects. This step requires terrain analysis, weather analysis and analysis of other characteristics of the battlefield. IPB should specifically specify human terrain analysis, how to analyze it and provide patterns for prediction.<sup>10</sup> In addition to designing a Pattern Analysis Wheel, Incident Overlay, and (priority intelligence requirements) PIRs for example, military intelligence personnel should possibly adopt some of the HTTs products such as social network mapping and creating a database of cultural traits.

The Human Terrain System, effectively employed in 2006, has demonstrated the great need for socio-cultural understanding. Human Terrain Teams are aiding brigades and regiments in Iraq and Afghanistan and influencing force protection. The Military Intelligence Corps can take these lessons learned from Human Terrain Teams and exploit them for intelligence collection. In addition to traditional forms of intelligence, socio-cultural intelligence is needed even more in a counterinsurgency fight. United States military leaders recognize that in our modern irregular warfare, victory is not solely a military victory. Instead, stability is the sought

after prize. At the heart of stability or political unrest are people's desires and expectations. If military intelligence professionals focus on the human terrain, it will enhance intelligence collection and consequently aid in the stabilization of Afghanistan and Iraq. By synthesizing social sciences and military intelligence, the United States military as a whole will benefit and aid countries towards stabilization in the process.

## End Notes

- 1 Benjamin C. Freakley, "Cultural Awareness and Combat Power," *Infantry* vol. 94, (2005): 1-2.
- 2 Jacob Kipp, Lester Grau, Karl Prinslow, Don Smith, "The Human Terrain System" *Military Review* (2006): 8-15.
- 3 Accessed from <http://humanterrainsystem.army.mil/> 21 November 2008.
- 4 Accessed from <http://humanterrainsystem.army.mil/> 21 November 2008.
- 5 Noah Shachtman, "Army Anthropologist's Controversial Culture Clash" *Wired*, 23 September 2008. Accessed from <http://blog.wired.com/defense/2008/09/controversial-a.html>.
- 6 Accessed from <http://humanterrainsystem.army.mil/> 21 November 2008.
- 7 Col. Martin P. Schweitzer, "Report before the House Armed Services Committee, Terrorism, and Unconventional Threats Sub-Committee and the Research and the Research & Education Subcommittee of the Science & Technology Committee, 24 April 2008, Washington, D.C.
- 8 Jacob Kipp, Lester Grau, Karl Prinslow, Don Smith, "The Human Terrain System" *Military Review* (2006): 8-15.
- 9 Jacob Kipp, Lester Grau, Karl Prinslow, Don Smith, "The Human Terrain System" *Military Review* (2006): 8-15.
- 10 FM 34-130



*2LT Lindsey Marie Champion was born and raised in Miami, Florida and attended from Carrollton School of the Sacred Heart for her secondary education. While in highschool, she played tennis and ran cross-country. A graduate of the United States Military Academy at West Point, LT Champion majored in Comparative Politics. At the academy, she participated in the Gospel Choir, Women's Cross-country and track, and Powerlifting. LT Champion is currently assigned as the assistant S2 to 3-82 General Support Aviation Battalion at Fort Bragg, NC.*

---

# Regression in Analysis

---

by 2LT Kevin Burke

*VanDemam Program paper*

In regression analysis, the goal is to determine the values of parameters for a function to best fit a set of data observations. Put another way, regression attempts to best describe what inputs result in a given output. Though there are many complex forms or regression models, the simplest is a linear regression model. This is the model I will use for illustration purposes. I do this solely for the purpose of building a basic understanding of regression analysis. One must realize, therefore, that the type of regression analysis that could prove useful to the intelligence community would also prove far more complex.

Take, for example, the value of a car. If one assumes that said value decreases by a constant amount each year after its purchase, as well as for each mile it is driven, the linear function “value = price – (x)age – (y)miles” would predict its value. In this equation, “value” is the market value of the car, “age” is how old the car is, and “miles” is the number of miles that the car has been driven since its purchase. “X” and “Y” represent the relationship between the value of a car and its age and mileage respectively. In this case, one would expect the relationship to be negative. That is to say, one would expect the value of a car to decrease as age and mileage increase.

In any analysis of this type, one must provide a data file which contains the values for the variables. In this example, each data record would need to contain three numbers: value, age, and miles. For this example, the classifieds section of a newspaper might be a valuable source of data. The most important thing to remember about data sets, though, is that size does matter. The more observations provided, the more accurate the analysis.

At this point, it may still be unclear as to how regression analysis can be used throughout different fields. For Economists, one may want to get a better understanding of the way families spend money. In this case, the dependent variable might be a family’s consumption expenditure and the independent variables might include the family’s income, the number of children in the family, the amount of debt held by the family, and other factors that may affect the family’s expenditures. For Sociologists, the interest may be in finding out what, if any, is the relationship between one’s social status and one’s occupation. Here, the independent variables might be inherent characteristics of one’s job such as pay, qualifications, education, etc. In the intelligence world, especially given the current conflicts, one might

be interested in determining what factors may or may not contribute to the emplacement of an IED.

Here, before I begin to lay out my initial equation, it seems quite important to point out two things. First, biases are an inevitability of everything we do. Whether it rears its head when one makes an assumption about the used car salesman in the ugly coat, or whether it’s found in the assumptions that an analyst makes about the enemy, they are always there. This, however, does not mean all hope is lost. Rather, one need only to recognize one’s biases, account for them, and move on. The point being that, even with biases, it is quite possible to provide quality analysis. Secondly, it is imperative that one thing be quite clear. I am not, in any way, arguing that regression analysis is the end-all be-all of analytical tools. It is not the magical key that unlocks the enemy’s secrets. It is not a discrete tool intended to be used by itself. And, above all else, it will not, under any circumstances, do the analysis for the user. Like anything else in the analyst’s toolkit, regression analysis will only aid the analyst in making better, more predictive conclusions. Nothing more!

That being said, one more thing must be brought to light: my biases. My combat experience, thus far, has been that of a lower-enlisted gunner in an infantry unit. Specifically, I spent the better part of a year driving very slowly through southwestern Baghdad clearing routes. Put another way, I spent a year trying to find IED’s before they found me. With that, one must realize that my proposed equation is very specific. Anyone who has spent anytime whatsoever in the area will realize that my equation is a very Baghdad-centric one. Again, though, that does not render it useless. Rather, it means only that the analysis tool I put forth cannot be used everywhere. Different areas, countries, enemies, etc will all require their own model. Just as the model used to fight the Russians during the Cold War contrasts dramatically with the model needed to fight an insurgency, so too does regression analysis require varying models for varying situations.

$$\mathbf{B = a S + c P + d T + E}$$

Where:

- S = socioeconomic status of an area
- P = previous IED activity
- T = time
- E = unattributed factors

Above is what I suggest to be a beginning to understanding IED emplacements in and around Baghdad. As stated previously, it is not intended to be the answer. It

is only put forth in order to encourage analysts to use regression models in their analysis.

To begin, it seems easiest to discuss the simplest of the variables. First, as is commonly known, it is often an enemy TTP to emplace an IED in a location that has had previous success. That is to say that the enemy, quite literally, often place a new IED in the crater formed by an earlier IED. Such was certainly my experience and, from talking to others, theirs as well. It seems like a very logical variable to be included.

The next simple variable is the “time” variable. Dusk and dawn, and not just with IED’s, is often the time of enemy attack. Therefore, it seems important to incorporate that common occurrence into the equation. For me, it seemed like something always went “boom” when we had the sunrise patrol. Also, though, the “time” variable would begin to account for dates and time of year. Mondays always seemed more dangerous than Fridays. Uncomfortable months (too hot and too cold) seemed safer than comfortable ones. Holidays always seemed a bit more dangerous. “Time” attempts to account for the fluctuations that happen according to the calendar and watch.

Lastly, “socioeconomic status” (SS) attempts to quantify that gut feeling that every soldier has about an area, about a “bad” area. I can’t recall one time ever being attacked, IED or otherwise, in a nice neighborhood. That’s not to say that it doesn’t happen, but it seems logical that it is far less likely to occur. In addition, unlike the previous variables, there is no single metric that comprises the data entry. On the contrary, the “SS” variable would certainly be a compound variable. That is, it would be a variable, one data entry, comprised of a series of

other measurements. For example, in constructing the “SS” variable, one might consider things like per capita income, reliability of public services, and the number of schools in an area. In constructing this variable, one would want to consider, or quantify, all of those things that make one neighborhood “worse” than another.

In closing, it seems essential to reiterate several key points, not only to remind those readers who have determined regression to be hogwash, but also to ensure that there be no mistake as to what role regression analysis can play in intelligence. Put simply, regression is nothing more than another tool available to the analyst. It is not, and should not be the analysis. Just as a pattern analysis wheel is nothing more than pretty shapes and colors if there is no analysis, so too is a regression model nothing more than a headache-causing jumble of numbers without solid theory and analysis behind it. Also, remember that a regression model is a very specific thing. While the intent is to create a model and analyze a data set in order to better predict, one must realize that, ultimately, the model only tells the analyst about that specific data set. It is up to the analyst, and those creating the models, to determine whether or not effective predictions can be made. Lastly, regardless of whether one understands regression a little bit or not at all, it is important to remember that the whole point is to make improvements. While the IED model presented above is clearly immature, incomplete, and overly simple, it is a beginning. “Good enough” is not a phrase that should ever enter the analyst’s lexicon. To do so is to put soldiers at risk willingly. Improvement, not perfection, is the goal, and the addition of regression analysis to the analyst’s toolkit would certainly be a vast improvement.



---

## Deterrence and Terrorism.

---

By 2LT Mitchell Suliman

*VanDemam Program paper*

Although deterrence appeared to be successful throughout the Cold War, its utility in the 21st century is highly problematic at best given the different conditions of our current War on Terror.<sup>1</sup> The purpose of this paper is to examine the state of deterrence now, to analyze both proponents and opponents of deterrence, and broadcast suggest a possible future for deterrence as applied to the military intelligence profession. It is important to note that deterrence is only one of the several strategies that can be used to counter combat terrorism. Other strategies include persuasion, economic aid, democratization, appeasement, and brute military force.<sup>2</sup> Given

the tragic September 11, 2001 attacks in America and the recent subsequent War on Terror, it is important to discuss the strategic role that deterrence plays (or should play) in U.S. counterterrorism policy. In response to 9/11, the Department of Defense assembled the National Defense University Task Force on Combating Terrorism to develop a strategy which would address the new deadlyemerging terrorist threat. Originally, the task force proposed a “3-D strategy” which had three goals: to defeat, deter, and diminish the enemy.<sup>3</sup> However, by the time the strategy was adopted, the word “deter” was replaced by “deny” and “defend.” As such, the final strategy issued in February 2003 called for a “4-D strategy” with the goals of to defeat, deny, diminish and defend against the adversary.<sup>4</sup> Although many may view this asThis may appear an insignificant substitution of words, this particular diction signifies the interaction

deterrence plays (or could play) on against terrorism. It is imperative this interaction is examined in depth as there are many schools of thought regarding the applicability of deterrence to counterterrorism efforts.

## **Against Deterrence**

In the aftermath of September 11th, many dismissed the applicability of deterrence in countering combating terrorism. The apparent inapplicability of deterrence has resonated throughout the Bush administration as well the U.S. national security strategy which states, “[t]raditional concepts of deterrence will not work against a terrorist enemy.”<sup>5</sup> As a result, there has been a shift from deterrent strategies of the Cold War to preemptive counterterrorism strategies of today.<sup>6</sup> There are several explanations for this shift away from deterrence. In a 2002 RAND report, Paul Davis and Brian Michael Jenkins write that “the concept of deterrence is both too limiting and too naïve to be applicable to the war on terrorism.”<sup>7</sup> Likewise, Richard Betts argues that deterrence has “limited efficacy...for modern counterterrorism.”<sup>8</sup> There are several explanations to why deterrence may be inapplicable or difficult in countering combating terrorism.

First, terrorist motivations are too strong. Arguably, the issue of terrorist motivation poses the greatest problem in implementing deterrence strategies.<sup>9</sup> Robert Pape argues that terrorists are extremely motivated as they are willing to die, and so not deterred by fear of punishment or of anything else.<sup>10</sup> Terrorism is difficult to combat, because individuals are motivated by religious and ideological beliefs. When highly motivated, terrorists are more willing to risk anything to accomplish their goal. As such, suicide terrorism and martyrdom play an important role. For example, Bin Laden and members of al-Qaeda may see themselves as prophets or at least as instruments of God’s will. They are no longer motivated by the preservation of life, but rather are motivated in pursuit of a particular image of Islam and “its crusade against the infidels.”<sup>11</sup> This intense motivation creates another problematic condition for deterrence strategies. The political goals of terrorist groups are ambiguous, broad, and unclear mainly due to their idealistic beliefs.<sup>12</sup> Given the motivation of terrorist operators, many analysts dismiss the concept of deterrence.

Second, terrorists are often labeled as being “irrational.” Therefore, terrorists do not value the cost-benefit analysis that is the foundation of deterrence. Some argue that this irrational behavior is exemplified by having no other purposes other than causing death and destruction.<sup>13</sup> This creates a problematic scenario as in which terrorists may not be concerned with the political advantages or further benefits that may result from their actions. Given the irrationality of terrorists, it is difficult

to develop effective responses or deterrent strategies as they may be useless due to the nature of the adversary. Additionally, it is extremely difficult to deter an adversary that prefers escalation regardless of the consequences.<sup>14</sup> Thus, the combination of extreme religious ideology coupled with extra-terrestrial potential rewards for martyrdom creates a sort of irrationality which renders deterrence ineffective and irrelevant.

Third, a practical problem for deterrence exists. Terrorists lack a return address and are usually difficult to find making retaliation difficult burdensome to execute.<sup>15</sup> This “return address problem” mitigates effective deterrence as it reduces the degree of leverage of certain types of threats.<sup>16</sup> Terrorist networks usually operate on a trans-national basis. As such, this problem crosses multiple borders which make reprisals difficult to “return to sender”.<sup>17</sup> A terrorist organization may lack specific territory, population, and infrastructure. The invisibility of terrorist networks makes deterrent strategies such as retaliation or punishment less credible. Given the difficulty of locating terrorists and the lack of a singular adversary, deterrence seems less likely to work against terrorism.

## **For Deterrence**

The claim that deterrence is ineffective and useless against terrorists is not a universal—to say the least—consensus. While many scholars and analysts conclude that deterrence is of little use against terrorists, some hold that the “death of deterrence” has been exaggerated and can remain a key tool in the war on terror.<sup>18</sup> The continual applicability of deterrence is exemplified in the Quadrennial Defense Review, the four year US defense planning document released in early 2006, which uses the word “deter” over fifty times referring to “tailored deterrence for rogue powers, terrorist networks and near-term competitors.”<sup>19</sup> It is clear, however, that an appreciation for the value of deterrence is growing with time. Therefore, it is imperative that a thorough examination of the applicability of deterrence logic as related to terrorism is conducted.

First, some argue that September 11 was not the event that triggered the ineffectiveness of deterrence; rather, the U.S. foreign policy throughout the 1980s and 1990s “failed to communicate to al-Qaeda that the U.S. was willing and able to inflict significant suffering on terrorist transgressors.”<sup>20</sup> As such, deterrence did not fail, but rather the United States failed to establish a credible and effective mechanism to deter al-Qaeda. This is also evident when President Bush noted in 2001 in an interview with the Washington Post that, “It was clear that bin Laden felt emboldened, and didn’t feel threatened by the United States.”<sup>21</sup> There are several examples of when the United States failed to retaliate against terror-

ists. Well known attacks such as, the 1993 World Trade Center bombings, the embassy bombings of 1998, and the bombing of the USS Cole in 2000 all went without retaliation and thus, lacked an effective deterrent mechanism. Unfortunately, the lack of retaliation did not go unnoticed by Osama bin Laden as he repeatedly labeled the United States as a “paper tiger”, a country more prone to growl than to bite.<sup>22</sup> Thus, it was not that deterrence was ineffective, but rather a credible deterrent response was not established in the first place.

Second, many analysts argue that terrorists can be deterred since most terrorist networks are hierarchical organizational structures. This structure allows terrorist organizations to have specific goals and strategies which best advance them and their ideology.<sup>23</sup> There are many actors of a terrorist group to include: leaders, religious figures, financiers, recruiters, and various state supporters. Deterrence may be possible against such entities that compromise and support the terrorist network.<sup>24</sup> Several responsibilities within an organization allow for different deterrent mechanisms to apply. Many in a terrorist network have the cost-benefit calculation necessary for the adversary to be deterred. Opponents of deterrence argue that terrorists who are willing to conduct a suicide attack are undeterrable due to the irrational nature of the adversary and despite the hierarchical structure of the organization. However, others argue that this irrational behavior proves deterrence applicable.

Third, many hold that terrorists are not completely irrational. Although terrorist organizations are likely to have both rational and irrational actors, deterrence can still be applicable. Deterrence only requires a sufficient influence of a cost-benefit framework. Robert Jervis argues that “Much less than a full rationality is needed for the main lines of [deterrence] theory to be valid.”<sup>25</sup> Since most terrorist organizations are hierarchical in nature, terrorists most likely have ordered goals and strategies. Richard Betts argues that terrorists resort to their “irrational” tactics as a strategic choice with no other means of advancing their cause.<sup>26</sup> Robert Pape furthers this argument through his study of suicide terrorism. He argues that suicide terrorism is an effective coercive tool and strategic tactic used against liberal democracies. as it was seen as the most effective coercive tool.<sup>27</sup> This recurring theme of rationality is sometimes confused with reasonability.

Thus, the notion of irrational enemies is not the problem of U.S. deterrence logic. Rather, it is the completely rational adversary who connects tools which contradict that of U.S. values and western norms, making their instruments unreasonable to the other party.<sup>28</sup> The strategic logic of the adversary coupled with the confusion

between reasonability and rationality allows deterrence to be a potential tool against terrorism.

## **Implications of Deterrence**

There are several significant implications of using a strategy of deterrence to counter combating terrorism. It is important to examine these implications as they may have an extraordinary impact on a nation’s practices, ideals, and beliefs. Many scholars argue that deterrence may be applicable to counter combating terrorism, but the implications of using such strategies would have an adverse impact on current norms. One such scholar, Uri Fisher, writes that “deterrence, as a strategic concept, is not inapplicable to defending against terrorism; however, the U.S. would face considerable legal and moral quandaries if it were to carry out the necessary policies to deter terrorists and their supporters.”<sup>29</sup> As such, it is important that these legal and moral quandaries are discussed. The levels of harshness and brutality that simple deterrent strategies require make it difficult for the United States to use as it would create incredible controversy over the morality and civility of such actions. U.S. foreign policy is well-known to be a reflection of the nation’s core values and beliefs. However, in order to deter terrorism, the U.S. would have to find it necessary to compromise certain values such as democracy that have guided foreign policy for many years. The inability to use deterrent strategies due to the moral implications also establishes a less credible authority to the adversary. If credibility is mitigated, then the U.S. will have a difficult time communicating a clear message against terrorist elements.<sup>30</sup> If the U.S. cannot establish a clear and credible message, it increases the difficulty of changing the decision-calculus of the terrorist adversary. Many argue that deterrence is still applicable against the current threat of terrorism without examining the actual policies the U.S. would have to adopt and pursue in order to deter the adversary. However, the implications of these deterrent policies would be great. Not only would these policies degrade the moral authority the U.S. currently holds, but also these policies would be viewed as hypocritical and discreditable in the international arena. Thus, it is not a dilemma of inapplicability, but rather a dilemma of use versus non-use.

Many argue that terrorist networks involve civilian targets, illegitimate targets, and unprepared targets. When terrorists can be labeled as unlawful combatants and outside the protection of just war doctrine of *jus in bello*, many questions arise. For instance, what actions and degree of lethality can be used against terrorists? Are there appropriate moral, ethical, and legal constraints that should be applied to a deterrence strategy?<sup>31</sup> These are critical questions which many argue have severe implications to the strategy when applied to terrorism.

## Policy Recommendations and Military Intelligence Application

It is a fact that there is no single solution or quick fixes to successfully counter combating terrorism. However, it is possible to specify more effective and less effective deterrent strategies at various levels and under different conditions that Military Intelligence professionals can use. The general policy must be adaptive, opportunistic, and multisided multidisciplinary for it to be effective. It is also important that intelligence and targeting no should no longer take the conventional approach of "search and destroy" methods in an attempt to deter terrorists.<sup>32</sup> The likely long-term consequences of such actions will result in a degradation of the American image and damage to American credibility abroad, a spur to expand terrorist networks, and continued loss of life. Although conventional methods of deterrence may not be the most effective, deterrence strategies can still be highly effective to critical elements of terrorist networks. As such, the analysis above lends suggests several conclusions for U.S. counterterrorism policy.

First, traditional targeting of nonpolitical means can deter various elements of terrorist networks. For this to be effective, it is imperative that adequate resources are devoted to deterrence. Resource allocation is important for these methods to deter terrorism because it is essential that the capability and will to use these resources is both credible and clearly communicated.<sup>33</sup> The continued pursuit of specific terrorists who conducted attacks will demonstrate the will to use force which will likely increase future deterrence success. Intelligence analysts should place a greater emphasis on terrorist financiers as they have targetable assets which are nonpolitical in nature. which increases the chances of being found.<sup>34</sup> Thus, a higher level of resource allocation devoted to deterrence will increase the likelihood of future success of deterrent strategies.

Second, intelligence professionals should apply deterrent strategies to specific courses of action, rather than on individuals alone. Deterring certain courses of action will send a credible message to terrorist groups not to partake in the certain action. This strategy will also prevent terrorists from cooperating with each other in order to achieve synergy.<sup>35</sup> Empirically, it is proven that terrorists "feel constraints, that they argue and plot among themselves, review and adapt strategies, worry about their perceived constituencies, and sometimes back away from tactics that seem to have gone too far."<sup>36</sup> The operational risks that terrorists may consider can easily be influenced by applying strategies to specific courses of action as opposed to individual terrorists. Since terrorism is a networked operation, deterring courses of action will most likely discourage that action all-together, while

deterring individuals might only spur more extremists. As Paul Davis and Brian Jenkins write, "Committed terrorists do not reform, but they do change actions, and that can be important."<sup>37</sup> Military action and threats may deter other organizations than the primary target, making deterrence a feasible option.

Third, the intelligence community can focus more on deterrence by denial strategies which can be used to decrease the coercive nature of terrorist attacks and the motivation to conduct these attacks. Both an offensive and denial strategy can be applied in conjunction with each other. For example, the United States acted on denial principles with large-scale, offensive efforts in Afghanistan and Iraq. Additionally, the United States has actively pursued rogue-state arsenals in an attempt to deny them access and capability.<sup>38</sup> As such, a defensive and denial strategy should be applied. The offensive strategy should never impend upon a defensive strategy nor should it draw resources from the defensive posture of the U.S.<sup>39</sup>

Fourth, military intelligence professionals on the ground should adopt and direct a strategy toward distancing and alienating specific audiences from terrorist organizations and activities. Influence tactics can be used to counter combating the terrorist message or technique just as much as it influences the local population. Additionally, direct efforts should be made to work through all available third parties to include the following: societies housing terrorist organizations, countries trusted by these host societies, and the United States' own allies.<sup>40</sup> This allows for a clearer message to be sent to terrorist organizations that many disapprove of their actions and are willing to apply deterrent strategies to minimize threats and attacks. Additionally, the message is more credible when several parties demonstrate the willingness to utilize their capabilities to combat terrorism. The incorporation of extremist groups into society is another goal that should be pursued as this will decrease the motivation of a terrorist's cause.

Fifth, the extension of ideological influence must be continued to combat extremists who aspire to conduct such attacks. However, this ideological influence does not and should never depend on armed forces. It can result from several other factors to include include the: the activities of multinational corporations, the influence of global media, international bodies and projects, and extraterritorial legislation.<sup>41</sup> A key to effective deterrence is extending the deterrent strategy and influence tactics to the society that supports the particular terrorist organization.

It is clear that there is not a single solution to the problem, but rather a multifaceted approach that is both adaptive and flexible by nature is necessary to combat

terrorism. Deterrent strategies are still necessary in the fight to say the least. Thus, our the approach must be composed of three essential components. First, the capability to achieve the desired effect must be attained. This can include anything to include: the use of force, denial strategies, defensive posture, influence tactics and cooperation efforts. Whatever the policy or strategy is, it must have the required capabilities. Secondly, the strategy must be credible. Credibility issues are raised when exertions have to be made for third parties, costs to include enforcement appear too high, or when the threats are too difficult to restrain.<sup>42</sup> The strategy must be credible in the eyes of the adversary in order for deterrence to work. Lastly, communication is essential to the policy. The threat, action, or strategy must be clearly and repeatedly communicated to the adversary. Communications may have to be constructed with several audiences in mind, and the possibility of misperceptions will need to be addressed.<sup>43</sup> Therefore, deterrence will remain effective given the right strategies and the incorporation of three main elements: capability, credibility, and communication.

## End Notes

- 1 Colin S. Gray, *Maintaining Effective Deterrence*, (Washington D.C.: Strategic Studies Institute, 2003), v.
- 2 Robert F. Trager and Dessislava P. Zagorcheva, "Deterring Terrorism: It Can Be Done," in *International Security*, Vol. 30, No. 3, (Winter 2005/06), 89.
- 3 Doron Almog, "Cumulative Deterrence and the War on Terrorism" in *Parameters*, Winter 2004, p., 14.
- 4 George W. Bush, *National Strategy for Combating Terrorism* (Washington: The White House, February 2003), p. 15.
- 5 George W. Bush, *The National Security Strategy of the United States of America* (Washington D.C.: U.S. Government Printing Office, 2002), 15.
- 6 Uri Fisher, "Deterrence, Terrorism, and American Values," in *Homeland Security Affairs*, Vol. 3, No. 1, (February 2007), 1.
- 7 Paul K. Davis and Brian Michael Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on al-Qaeda*, (Santa Monica: RAND, 2002), xviii.
- 8 Richard K. Betts, "The Soft Underbelly of American Primacy: Tactical Advantages of Terror" in *September 11, Terrorist Attacks, and U.S. Foreign Policy*, ed. Demetrios James Caraley, (New York: Academy of Political Science, 2002), 46.
- 9 Trager and Zagorcheva, 94.
- 10 Robert A. Pape, *Dying to Win: The Strategic Logic of Suicide Terrorism*, (New York: Random House, 2005), 5.
- 11 Davis and Jenkins, 4.
- 12 Fisher, 1.
- 13 Lawrence Freedman, *Deterrence*, (Cambridge: Polity Press, 2004), 123.
- 14 Daniel Whiteneck, "Deterring Terrorists: Thoughts on a Framework," in *The Washington Quarterly*, Vol. 28, No. 3, (Summer 2005), 187.

- 15 Betts, 45.
- 16 Trager and Zagorcheva, 108.
- 17 Fisher, 1.
- 18 Fisher, 1.
- 19 James H. Lebovic, *Deterring International Terrorism and Rogue States: US National Security Policy After 9/11*, (New York: Routledge, 2007), 8.
- 20 Fisher, 1.
- 21 Ibid, 2.
- 22 Ibid.
- 23 Martha Crenshaw, "The Causes of Terrorism," in *International Terrorism: Characteristics, Causes, Controls*, ed. Charles W. Kegley, (New York: St. Martins, 1990), 117.
- 24 Fisher, 2.
- 25 Jervis, "Deterrence Theory Revisited," 299.
- 26 Betts, 45.
- 27 Pape, 44-45.
- 28 Keith B. Payne, *The Fallacies of Cold War Deterrence and a New Direction*, (Lexington: The University Press of Kentucky, 2001), 10.
- 29 Fisher, 1.
- 30 Ibid, 2.
- 31 Harvey Rishikof, "Morality, Ethics, and Law in the Global War on Terrorism (The Long War)", in *Countering Terrorism and Insurgency in the 21st Century: International Perspectives*, ed. James J.F. Forest, (West Port: Praeger Security International, 2007), p. 107.
- 32 Niel J. Smelser and Faith Mitchell, *Discouraging Terrorism: Some Implications of 9/11*, (Washington D.C.: The National Academies Press, 2002), p. 31.
- 33 Trager and Zagorcheva, 120.
- 34 Ibid.
- 35 Ibid.
- 36 Davis and Jenkins, 59.
- 37 Ibid, 60.
- 38 Lebovic, 179.
- 39 Ibid, 180.
- 40 Smelser and Mitchell, 31.
- 41 Freedman, 127.
- 42 Freedman, 130.
- 43 Ibid.

*2LT Suliman was born in Sugar Land, TX, and grew up in a suburb of Houston. In May of 2004 I graduated High School and went on to the US Military Academy. He earned a Bachelors of Science in International Relations (with Honors) in May of 2004. While at West Point, he was on the debate team for four years. Upon graduation he was commissioned into Military Intelligence. He is currently assigned to 4ID and will be deploying in support of 4th AV BDE.*



---

# Intelligence “Reach Back” Only Works if We “Reach Forward”

---

by CAPT Paul Becker, USN

## What Have We Observed, What Have We Learned?

The War on Terror is largely taking place in the Central Command’s Area of Responsibility (CENTCOM AOR) but it’s not just CENTCOM’s fight. It’s the nation’s fight and that makes it the Navy’s and Naval Intelligence’s fight as well. For the foreseeable future the War on Terror will be the central objective of the United States.<sup>1</sup> Combat operations in the CENTCOM AOR that are an element of this war are referred to as “The Current Fight,” and contributing to this fight is a top priority for the Chief of Naval Operations and Director of Naval Intelligence. The Current Fight is a joint, combined and largely ground fight with Navy and Naval Intelligence contributing from the sea in accordance with the tenets of our Maritime Strategy, and also ashore in forward battle spaces with Special Task Forces and in Command Headquarters.

For the past seven years I’ve experienced first hand the positive impact that Intelligence Individual Augmentees (IAs) are achieving at the vanguard of The Current Fight. By defining intelligence success as a commander’s or decision maker’s satisfaction that their intelligence team is providing knowledge resulting in rapid/decisive operations, I’ve observed our greatest intelligence successes take place when true Subject Matter Experts (SMEs) are embedded alongside operators at forward locations, and not just randomly selected IA’s electronically retrieving and sharing knowledge from the United States. An intelligence professional’s main armament is knowledge of the enemy. Basic knowledge of how to utilize the intelligence “system” is helpful but is not the same as a “SME.” Simply sending forward enthusiastic and bright, but inexperienced intelligence volunteers from a Theater’s Joint Intelligence Center or a Service’s National Intelligence Center who electronically “reach back” to their parent command is insufficient in providing war fighters what they want and need to win: a readily accessible deep understanding of the enemy from those with first-hand knowledge of the battlespace.

A key lesson learned from intelligence operations in The Current Fight is that the quality of intelligence reach back is directly proportional to the quality of personnel sent forward. Intelligence “REACH BACK” works best if we enable it with experts forward who know how to draw on and leverage resources and infrastructure from their higher Headquarters and coach others on scene ... in fact we must “REACH FORWARD” to achieve desired

combat effects. When we start thinking to ourselves at a Theater or Service Intelligence HQ that such individuals are too valuable to go forward ... then we’ve found the right people! The Naval Intelligence community has been “reaching forward” in The Current Fight with great success ... and we must apply this lesson elsewhere when executing The Maritime Strategy to ensure Naval Intelligence’s prominence and dominance in all theaters during peace, crisis and war.

## How Do We Adapt These Lessons To The Navy’s Maritime Strategy?

Naval Intelligence personnel serving forward in The Current Fight succeed in large part because of our Community’s longstanding requirement to be “specialists in the profession of intelligence,”<sup>2</sup> applying core skills of analysis, targeting, collections and signals intelligence with flexibility and speed to dynamic problem sets from Balad to Bagram to Bushehr, from the Suez to Strait of Hormuz to Shatt Al Arab, from Kabul to Kandahar to Kenya. Our Community’s strength of three-dimensional operational thinking (historically applied against threats beneath the seas, on the surface and in the air) is well suited against irregular/unconventional threats with adversaries organized as networks and not nations. Naval Intelligence is similarly networked with National Intelligence Agencies, which are a subset of what the Maritime Strategy refers to “elements of national power.”<sup>3</sup> These linkages must not only originate from analysts at intelligence centers in the United States, but from forward joint combat commands/staffs and regional Maritime Headquarters with Maritime Operations Centers (MHQ/MOC).

An essential element of implementing the Maritime Strategy is “forward presence.” While forward presence refers primarily to Task Forces/Groups/Units and their associated platforms, the desired effect is an operational understanding of the local environment and the necessary experience to quickly succeed in any crisis or combat scenario. In this era of Fourth Generation warfare when knowledge, speed and precision are more important than mass, fires and maneuver on the battlefield, a deep understanding of an adversary’s intent and capabilities is a key component of the Maritime Strategy’s power projection principle. Thus, the practice of having our best intelligence personnel forward in The Current Fight, or in a MHQ/MOC that focuses on potential threats to Navy and Nation from areas such as the South China or Arabian Gulf, is a practice that is fully aligned with Naval Intelligence’s mission: “Enable Decision Superiority for our commanders and operational forces by harmonizing Navy’s Intelligence and Information Operations efforts to achieve a penetrating knowledge of adversaries and a profound understanding of the maritime environment.”

By regularly reaching forward with SMEs the Naval Intelligence Community can enhance a MHQ/MOC's capacity to achieve success across the full spectrum of missions to include enhanced Maritime Domain Awareness by globally networking with other elements of national [intelligence] power. This in turn achieves another MHQ/MOC objective; alignment with other services through the implementation of their best practices.<sup>4</sup> "Reach Forward" truly applies here. For the past several years the Joint Intelligence Center Central Command (JICCENT) and other Special Operations Commands have been reaching forward with their best personnel ... some senior, some junior, but always the best. Not just Counter-Terrorist analysts into Iraq and Afghanistan, but regional analysts to Embassies and the Combined Joint Task Force Horn of Africa. To maintain a cycle of continuous forward presence, JICCENT adopted and applied the Special Forces best practice of four month deployments; an optimum duration given the 1) extraordinary hours applied to intelligence problem sets when forward, and 2) there is no "start up cost" to get an SME up to speed on a local issue. Due to limited numbers (and relatively short 1-3 years tours) of uniformed intelligence personnel in certain commands, the majority of SMEs forward in The Current Fight are DoD civilian and long-term contractors all of whom have deployment mobility orders written into their contracts affording them the opportunity to serve wherever the action is in this time of war (The 2008 National Defense Strategy states, "The United States must improve its ability to deploy civilian expertise rapidly ... greater civilian participation is necessary to both make military operations successful and relieve stress on the men and women of the armed forces"<sup>5</sup>). With a roughly "one in four" rotation cycle (i.e. four months forward, twelve months back home), SMEs who return from forward rotations continue to work the same target sets at home, training others and thereby building analytic "bench strength" for enduring focus areas.

## **Naval Intelligence's Past, Present And Future**

Naval Intelligence has a tradition of reaching far forward to support operations. Commands such as the Cold War era Pacific, Atlantic and European Fleet Area Support Teams (FAST) are such examples. The Naval Intelligence community still provides Information Warfare (formerly "Cryptologic") Direct Support Elements (DSE) to platforms deployed around the globe that collect and analyze intelligence which contributes to a penetrating knowledge of current and future threats. Today the Office of Naval Intelligence reaches forward to the Fleet by providing Acoustic Intelligence (ACINT) and Fleet Imagery Support Team (FIST) augmentees to Strike Group and Fleet staffs, Tactical Intelligence Specialist

Teams (TISTs) from TRIDENT's Naval Special Warfare Directorate to Iraq/Afghanistan/Horn of Africa, and Liaison Officers (LNOs) to the Fifth and Sixth Fleets and Fleet Forces Command. The Office of Naval Intelligence, as well as all Theater Joint Intelligence Centers, should also adapt a best intelligence practice from The Current Fight and expand their reach forward by rotating additional SMEs, civilian and military – for approximately four months – to all MHQ/MOCs. Because there is no one template for the size and organization of a MHQ/MOC, and because ONI already maintains a healthy footprint of personnel certain locations like the Pacific Fleet MHQ/MOC, the contribution in both number and type of analysts should be appropriately tailored to the regional mission. In keeping with best practices from The Current Fight, these maritime analysts should not be personnel who are sent to simply fill a manning requirement, but knowledgeable professionals who can both contribute and help train the relatively transient forward uniformed personnel, then return home to impart their refreshed operational knowledge with colleagues.

"Reach Forward" provides a unique opportunity for Naval Intelligence to build on our tradition of operational relevancy within our uniformed and civilian workforce for the short and long term. Strive as we may, U.S. Naval and Joint forces will never have complete knowledge of the battlespace ... but we must have more knowledge than our adversaries, both current and potential. "How" we focus our efforts is as essential as "Where" we focus our efforts in modern warfare, and a rotation of our best analysts forward - where operations and intelligence come together in Fusion Centers, afloat and ashore – addresses this need. It was slightly more than 100 years ago that U.S. Navy legend, Admiral George Dewey, declared after his victory at Manila Bay, "As valuable as my training [ashore and in class] was, it was poor schooling beside that of serving for Admiral David Farragut in time of war."<sup>6</sup> Reaching forward today will provide the current generation of Naval Intelligence professionals a similar opportunity to serve, learn and succeed alongside commanders and decision makers who will be our nation's Admirals and Generals of tomorrow.

## **Conclusion**

The Maritime Strategy focuses on opportunities, not threats.<sup>7</sup> Applying "Reach Forward" lessons from the joint intelligence community in The Current Fight provides an opportunity for Naval Intelligence professionals to build on our community's tradition of operational relevance through expanded participation in regional MHQs/MOCs. Such participation is aligned with the Maritime Strategy's "Forward Presence" principle and MHQ/MOC's guidance to incorporate best practices

---

# Integration of Psychology into Intelligence Production

---

2LT Andrew Oracz

*VanDeman Program paper*

The current intelligence preparation of the battlefield procedure is an exhaustive and meticulous task of evaluating every aspect of the battlefield and attempting to deduce an enemy's course of action based on previously disseminated information regarding his doctrine and tactics. In evaluating the enemy, we often fail to look at the core of his nature. Insurgents do not strictly follow any particular doctrine in order to prevent themselves being locked into predictable tactics that can be overcome. The unexpected event, or "black swan," that comes as a surprise has no foundation in previous engagements or historical tendencies. If intelligence analysts are better familiarized with the psychological underpinnings of the enemy's nature, they are better prepared to understand his actions and intents. Ultimately, the aim is to gain a better understanding of what makes the enemy "tick."

In addition to overcoming the psychological obstacle of trying to think like the enemy, contemporary analysts would benefit from having an enhanced perspective of their own thought processes. Certain characteristics are intrinsic to all analysts and everyone is biased and subjective on some level. Better understanding of human psychology will aid in recognizing the presence and influence of opinion on analysis.

Presently, the training that intelligence officers receive at MIBOLC does not include much material on the machinations of human thinking. Analysts examine the enemy through the lens of Intelligence Preparation of the Battlefield (IPB). The four step process defines the battlefield environment, describes its effects, and then evaluates the threat, taking into account the enemy's capabilities, disposition, composition and preferred tactics. The final step is developing possible courses of action based on the previously identified information. <sup>1</sup> Throughout the procedure, the enemy mentality is not explicitly engaged. Threat courses of action are based on previously observed tactics and techniques and what the enemy prefers to do historically. In our present conflict the enemy is specifically adapted to be tactically flexible and thus avoid demonstrating historic tendencies. Al-Qaeda has deliberately designed their training regimen to be experimental and ever evolving. Contrary to US instructors that are locked into training doctrine, enemy combatants like those of Al-Qaeda are constantly improving or shifting their tactics, techniques, and procedures. <sup>2</sup>

from sister services and network with appropriate elements of national power. It takes enormous resources to gain and maintain a deep knowledge of our current adversaries and potential future threats. There are always personnel, financial and opportunity costs associated with any intelligence effort forward, but the costs are worth it for Naval Intelligence to remain "World Class." Throughout this essay I've referenced lessons learned from our nation's involvement in The Current Fight, but lessons learned from World War II and The Cold War apply as well ... Where were our best analysts then, forward or in the rear? "Both," is the correct answer, but "the best of the best" were always rotating forward to overseas Fleet Ocean Surveillance Information Centers/Facilities (FOSICs/FOSIFs) and afloat assignments which afforded the greatest opportunities to observe, analyze and engage the threat. Defeating today's threats and developing an unmatched level of knowledge against potential threats of tomorrow takes pressure, patience and participation forward. There's never been a more important time to be a part of a Naval Intelligence Team "reaching forward" to achieve success.

## End Notes

1. "The National Defense Strategy," Department of Defense, July 2008, p.7.
2. "DNI Update: Intelligence – The Profession of Specialists," July 22, 2008.
3. A Cooperative Strategy For 21ST Century Seapower, Department Of The Navy, October 2007.
4. "Rhumb Lines: Maritime Headquarters with Maritime Operations Center (MHQ with MOC)," Navy Office of Information, March 7, 2007.
5. "The National Defense Strategy," p. 17.
6. Leadership Embodied: The Secrets of Success of the Most Effective Navy and Marine Corps Leaders, edited by LTCOL Joseph J. Thomas, USMC, United States Naval Institute Press, p. 44.
7. A Cooperative Strategy For 21ST Century Seapower.



*CPT Paul Becker, USN, is a MICA Member and Joint Intelligence Center Central Command (JICCENT) Commander.*

*This article was selected as the U.S. Naval Institute's 2008 Naval Intelligence Essay Contest winner and will also appear in a future issue of "Naval Intelligence Professionals Quarterly" magazine. While CAPT Becker's article was written with an orientation toward the Naval Intelligence community, the concept of "intelligence reach back / reach forward" has universal application for military and civilian intelligence professionals.*

One of the greatest shortcomings in attempting to predict an enemy's future actions based on previous engagements is the inability to foresee the "black swan." A black swan event is an outlier or event that is beyond the realm of normal expectations. It is simply a surprise because it is nothing like what has been experienced in the past. The attack on the World Trade Center and Pentagon on September 11, 2001 can be deemed a black swan. Its very unexpected nature helps facilitate the conditions for it to occur. That is to say had there been any expectations of such an attack there would have been counter-measure in place to prevent it.<sup>3</sup> Indeed, future terrorist attacks will aim to take on the shape of the black swan and strike where least expected.

To further complicate the conundrum of attempting to predict enemy behaviors, we must also overcome the notion that the enemy has a similar mindset to our own. The attacks on September 11th clearly demonstrated that terrorists of the militant Islamic breed do not hold to the same social norms, laws, or morals that we do. The act of committing suicide in effort to kill innocent civilians on a large scale is morally reprehensible and unimaginable, yet it is a tactic that is perpetrated with regularity in the Middle-East. During the Iran-Iraq war young children were sent to clear minefields while holding plastic keys to heaven.<sup>4</sup> How does the enemy mentally justify such actions? The ability to understand and predict enemy behaviors is not only dependent on knowing capabilities, but also understanding their moral boundaries. The perplexities of enemy behavior require a great deal of imagination and creativity to replicate. However, analysts need to develop predictions with the enemy's mindset, not their own.

Several reasons identified for intelligence failure are rooted in psychological pitfalls. Some of these categories described by Paul Reynolds in his article "Long History of Intelligence Failures," include overestimation, underestimation, complacency and mirror imaging. In each case, analytical predictions project internal biases on to the enemy. Overestimates determine the threat is greater than actuality, and underestimates deduce the enemy is not capable of doing something. The Battle of the Bulge came as a surprise because no one predicted enemy travel through the Ardennes Forrest as it was too dense through which to mount an offensive. This occurrence of mirror imaging occurred because intelligence analysis adapted the enemy course of action to friendly capabilities.<sup>5</sup> Predictive analysis of current terrorist threats must overcome the tendency to project friendly capabilities on to the enemy, even if those capabilities are representative of moral paradigms. Analysts must be able to surrender their bias of conscience.

Psychology of Intelligence Analysis by Richards J. Heuer examines the many psychological impediments

to intelligence analysis. Heuer points out that every analyst will bring their own subjective opinions and bias into their production of intelligence. Furthermore, many analysts are not able to rapidly incorporate abstract concepts into conventional problems, or fail to approach abstract problems with an abstract mindset. <sup>6</sup> Ultimately, a better understanding of psychology will help analysts better understand themselves and overcome obstacles like these.

The first phase of psychological adaptation to intelligence analysis is incorporating a block of instruction on introductory psychology into the intelligence basic officer leader's course. The recommended reading accompanying this block of instruction is Psychology in Action by Karen Huffman and Psychology of Intelligence Analysis by Heuer. It would best be placed in to the current training schedule just before classes on cultural awareness. Providing students with the basic tools of comprehension for complex insurgent behavior prior to engaging the mind set of the militant Muslim will allow for enhanced exploration of cognitive and emotive faculties that drive the threat to operate the way they do.

Following a brief exposition of basic human psychology, analysts can begin to apply those fundamentals to real world situations through case studies and selected readings. Based on their understanding of Middle Eastern culture in conjunction with the knowledge gained of the evolution of the militant Muslim through readings, students can begin to develop their own model for insurgent behavior.

Psychology and predictive analysis do not readily lend themselves as topics that can be testable in a simple GO/NO GO fashion. They are less of a simple dichotomy and more so a subject matter that is best suited for practical exercises. Students would explore the enemy mind through case studies provided by readings. The instructional block would culminate with scenarios in which students would have the opportunity to explore a situation through the enemy perspective. The focus is less at driving towards developing a "right" answer and more towards fostering creativity. The objective is to integrate what the analyst knows about the enemy, how they think the enemy thinks, and produce a prediction.

Ultimately, intelligence analysts would have a more positive footing inside the enemy's head and their own. Rather than question the moral nature of enemy behavior, analysts will be able to identify with enemy motivations and work within the paradigms of enemy cognitive patterns and behaviors. Intelligence work is not a 100% process. However, with a better understanding of human nature and the cultural implications of the contemporary operating environment, analysts will be better prepared to predict the next black swan.

Given that psychology is an often overlooked topic in predictive analysis, an increased amount of instruction would facilitate greater creativity. Analysts need to overcome their own psychological obstacles in developing intelligence that is objective and unbiased. Removing these inherent obstructions and increasing familiarization with enemy mentality will promote improved predictive analysis. In this era of unconventional warfare, creativity in analysis is paramount. Providing psychological training for analysts would only add another tool for cultivating that creativity. Improved analysis of the enemy from this mindset will better prepare intelligence professionals for predicting the next black swan.

## Conclusion

—Intelligence preparation of the Battlefield does not readily incorporate psychological analysis

—In addition to understanding the enemy better, analysts must better understand themselves to overcome personal weaknesses.

—Increased familiarization with enemy psychology and development of behavioral models will facilitate enhanced predictive analysis.

“If you know the enemy and know yourself, you need not fear the results of a hundred battles”  
—Sun Tzu

## Bibliography

- FM 34-130. Washington DC: Headquarters, Department of the Army, 1994.
- Aslan, Reza. No god but God: The Origins, Evolution and Future of Islam. New York : Random House Trade Paperbacks, 2006.
- Heuer, Richards J. Jr.. Psychology of Intelligence Analysis. Central Intelligence Agency : Center for the Study of Intelligence, 1999.
- Poole, H. John. Tactics of the Crescent Moon: Militant Muslim Combat Methods. Emerald Isle: Posterity Press, 2004.
- Reynolds, Paul. “Long History of Intelligence Failures,” BBC NEWS 2004.
- Taleb, Nassim Nicholas. “Learning to Expect the Unexpected,” Edge: The Third Culture 2004.

## End Notes

- 1 FM 34-130 (Washington DC: Headquarters, Department of the Army, 1994), 1.1-1.5
- 2 H. John Poole, Tactics of the Crescent Moon: Militant Muslim Combat Methods (Emerald Isle: Posterity Press, 2004), 179-180
- 3 Nassim Nicholas Taleb, “Learning to Expect the Unexpected,” Edge: The Third Culture (2004): 2-5
- 4 Reza Aslan, No god but God: The Origins, Evolution and Future of Islam (New York : Random House Trade Paperbacks, 2006), 245-255
- 5 Paul Reynolds, “Long History of Intelligence Failures,” BBC NEWS (2004): 1-3
- 6 Richards J. Heuer Jr., Psychology of Intelligence Analysis (Central Intelligence Agency : Center for the Study of Intelligence, 1999), 111-126

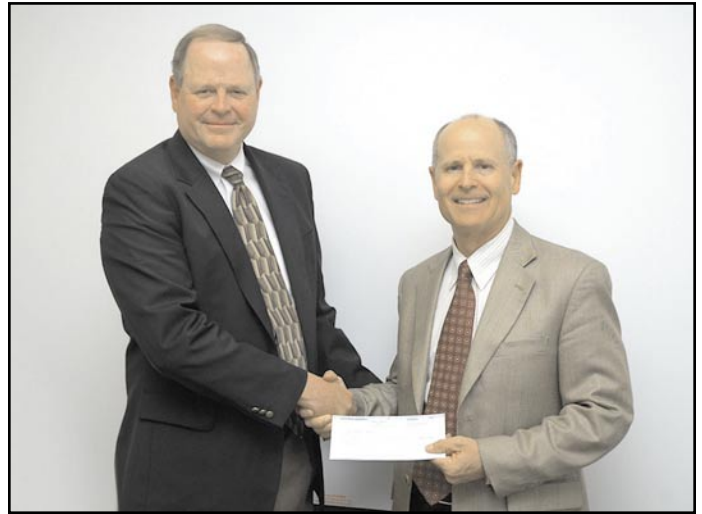


---

## MICA News

---

### Northrop Grumman makes scholarship donation



“Mr. Steve Pedigo of Northrop Grumman presents a donation of \$1,000 to the MICA scholarship fund to National President Larry Bruns. Northrop Grumman continues to be a significant corporate member of MICA and its generosity and support are very much appreciated by all members of the association.”

---

## Chapter News

---

### 3ID leaders visit MI Group, speak at local MICA luncheon—Fort Gordon

SSG Christopher Fincham

*116th Military Intelligence Group*

Fort Gordon military intelligence Soldiers gathered at the Gordon Club recently to enjoy lunch while building relationships and professional acquaintances. The lunch also served as an opportunity to glean knowledge from the guest speakers, the 3rd Infantry Division commander and members of his staff.

Maj. Gen. Tony Cucolo, 3ID commander, along with Brig. Gen. Thomas Vandal, 3ID deputy commander for support and Lt. Col. Mike Marti, the division’s intelligence officer, spoke to the members of the Master’s Chapter of the Military Intelligence Corps Association Jan. 30, during his visit to the 116th MI Group.

“We have a unique opportunity,” said Lt. Col. David May, the 206th MI Battalion commander and president of the local Masters MICA chapter. “To have the 3ID



leadership here to talk to our organization about the tactical war fighter expectations of MI professionals.”

“For my intel professionals – and this is rank immaterial, specialty immaterial – intel will drive everything that I do,” said Cucolo. “You are absolutely critical to my operations. It all starts with the reflexive competence that you all bring to your job.”

Vandal offered his perspective as a fire support and field artillery officer, to explain why MI is absolutely critical to the war fighter.

“As a professional ‘targeteer,’ I’ve got some challenges. One is, understanding the maneuver commander and how to integrate firers, both lethal and non lethal,” said Vandal. “We can’t get our job done without the support and analysis that you all provide. Likewise what you provide is absolutely invaluable to maneuver commanders. A lot of times you are the unsung heroes.”

“Although we don’t sing your praise often enough, you’ve got to understand how important you are to the success of every unit at every level,” Vandal said.

The 3ID leaders also took time to impress upon the MI professionals the importance and benefits of being involved in professional associations like MICA

Vandal encouraged everyone, regardless of rank or level of seniority, to participate in a professional organization.

“[MICA] is an example of a professional network, and as you become more senior, you will see the value of these networks. Not only the professional exchanges, but the networking, proves to be invaluable,” said Vandal.

Cucolo echoed his deputy’s statement saying that, “there are great benefits to joining organizations like this. Do not underestimate the social aspect of being a member of something like the Military Intelligence Corps Association. Getting peer-to-peer contact, meeting colleagues ... you will be on some battlefield, on some headset, and on the other end will be someone that you know.”

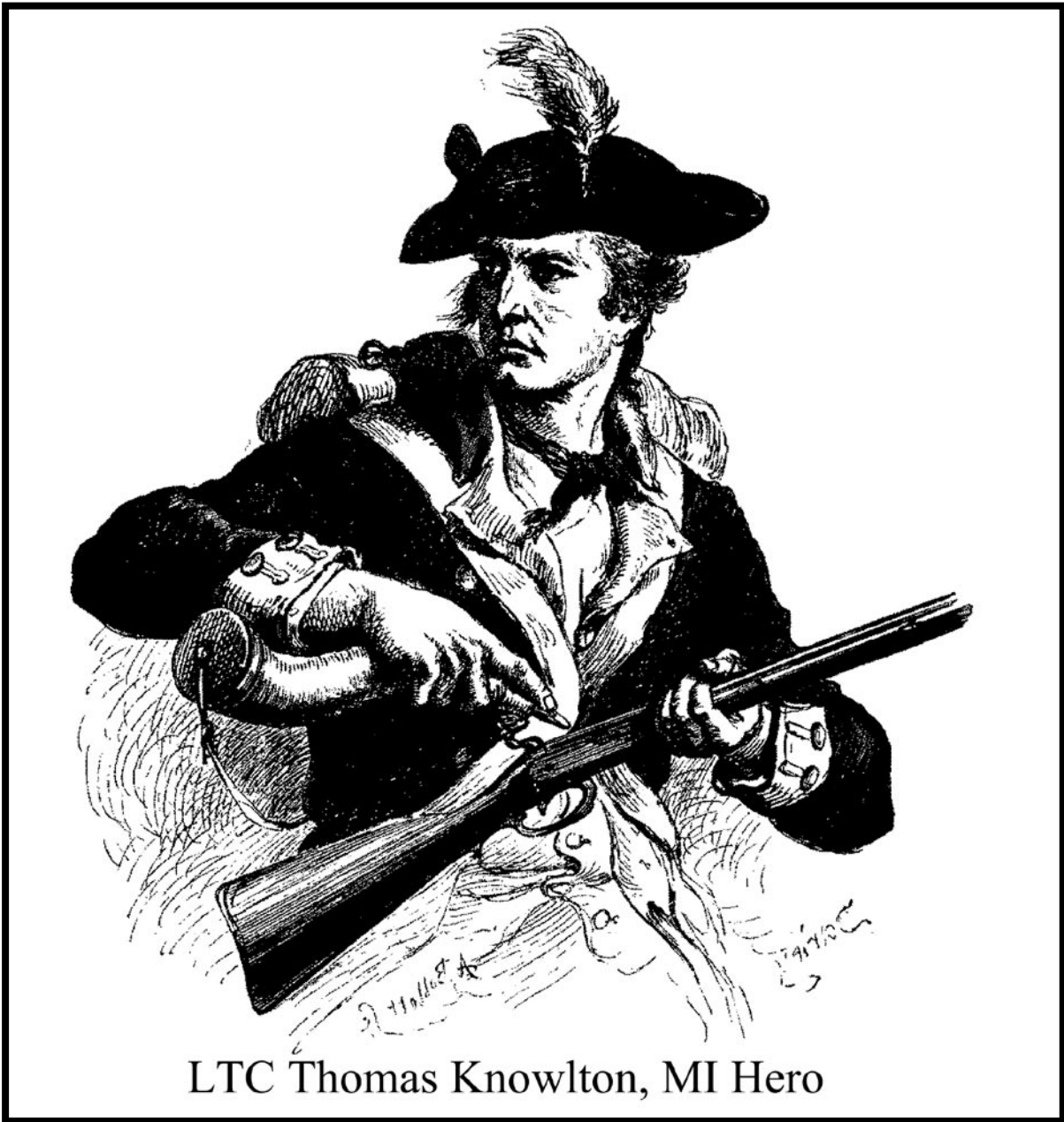
He went on to offer insights that he has garnered during his nearly 30 years of service.

“You will get instant credibility with all of the different people who you interface with if you are a professional Soldier. Do not let the unique requirements of your skill set drive you away from courtesy, bearing, your proficiency with your weapon, your physical fitness. Your credibility – the unspoken credibility – is those outward indicators of discipline,” explained Cucolo.

“So if you want a tip on instant credibility – never let slip those outward indicators of discipline that make you a professional Soldier,” Cucolo said.

As the Soldiers of 3ID prepare to deploy again in support of Operations Iraqi Freedom and Enduring Freedom, Cucolo stressed the importance of looking “beyond just the range of your M16” and ensured the MI Soldiers understood the important role that they will play in the ongoing War on Terrorism.

“The intel war fighting function has gotten so complex and so technical that sometimes you all seem like monks to us – the only people that understand the chanting of monks are other monks,” Cucolo said. “Show us how it works, how it fits. Relate it in terms we understand. You are our experts, and we’ll look to you.”



LTC Thomas Knowlton, MI Hero

***THE VANGUARD***

Military Intelligence Corps Association  
P.O. Box 13020  
Fort Huachuca, AZ 85670-3020

NONPROFIT ORG  
US POSTAGE PAID  
SIERRA VISTA, AZ  
PERMIT NO. 154

ADDRESS SERVICE REQUESTED