MILITARY INTELLIGENCE

PB 34-05-4
Volume 31 Number 4
October-December 2005

Purpose: The U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) publishes the ***Military Intelligence Professional Bulletin*** (**MIPB**) quarterly under the provisions of ***AR 25-30***. ***MIPB*** presents information designed to keep intelligence professionals informed of current and emerging developments within the field and provides an open forum in which ideas; concepts; tactics, techniques, and procedures; historical perspectives; problems and solutions, etc. can be exchanged and discussed for purposes of professional development.

Disclaimer: Views expressed are those of the authors and not those of the Department of Defense or its elements. The contents do not necessarily reflect official U.S. Army positions and do not change or supersede information in any other U.S. Army publications.

Contact Information for ***MIPB*** is on page 64.

FEATURES

DEPARTMENTS

By order of the Secretary of the Army:
Official:

Sandra R. Riley

SANDRA R. RILEY
Administrative Assistant to the Secretary of the Army
0603904

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Always Out Front

by Major General Barbara G. Fast
Commanding General, U.S. Army Intelligence Center and Fort Huachuca

Open Source Intelligence

The U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH), with the encouragement and support of the Army Deputy Chief of Staff for Intelligence, is creating a new Army intelligence discipline called Open Source Intelligence (OSINT). This new discipline recognizes the importance of public information; the need for a systematic approach to its collection, processing, and analysis; and its value in multidiscipline intelligence operations.

To facilitate the integration of the OSINT discipline into operations and training, USAIC&FH is developing an interim field manual (FMI) on OSINT. The manual, **FMI 2-22.9, Open Source Intelligence**, will provide interim tactics, techniques, and procedures (TTPs) on how to plan OSINT operations; collect and process publicly available information; and produce OSINT.

What does this new discipline mean to U.S. Army intelligence? OSINT operations are integral to Army intelligence operations. Publicly available information is the foundation upon which all intelligence operations build to develop all-source intelligence that supports situational understanding and decisive action. The availability, depth, and range of publicly available information enables intelligence organizations to satisfy intelligence requirements without the use of specialized human or technical means of collection. OSINT operations support other intelligence, surveillance, and reconnaissance (ISR) efforts by providing information that focuses collection and enhances production.

As part of an all-source intelligence effort, the use and integration of OSINT ensures that decisionmakers have the benefit of all available information. In short, OSINT as part of an integrated and balanced intelligence effort ensures that decisionmakers at all levels have the benefit of all sources of information.

American military professionals have collected, translated, and studied articles, books, and periodicals to gain knowledge and understanding of foreign lands and armies for over 200 years. The value of publicly available information as a source of intelligence has, however, often been overlooked in Army intelligence operations. The development of FMI 2-22.9 provides a catalyst for renewing the Army's awareness of the value of open sources; establishing a common understanding of OSINT, and developing systematic approaches to the collection, processing, and analysis of publicly available information.

Although readily available, the exponential growth in computer technology and the Internet over the past two decades has placed more public information and processing power at the finger tips of soldiers than at any time in our past. A body of knowledge on culture, economics, geography, military affairs, and politics that was once the domain of "grey-beard" scholars now rests in the hands of high school graduates.

For intelligence personnel, this combination of technology and information enables them to access a large body of information that they need to answer their unit's intelligence requirements. As the following quote illustrates, our over-reliance on classified databases and technical means of collection has often left our soldiers uninformed and ill-prepared to capitalize on the huge reservoir of unclassified information available from open sources.

I am deploying to El Salvador in a few months, and will be serving as the S-2 NCOIC for the task force there. I need to put together some information for the Task Force Commander on the country and the situation there. Although I have served in Operation IRAQI FREEDOM 1, I have no idea how to go about this, for

(Continued on page 4)

CSM Forum

by Command Sergeant Major Franklin A. Saunders
Command Sergeant Major, U.S. Army Intelligence Center and Fort Huahcuca

MI SOLDIER Update

I would like to open by stating that the sharing of information among Military Intelligence (MI) professionals is very important within our ranks. In an effort to enhance this ability, the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) has created the Intelligence Center Online Network (ICON) at https://icon.army.mil. At the ICON portal you will find links to many sites to include the Staff and Faculty Development Division, the MI Officer Basic Course, the Staff Weather Officer Course, the Office of the Chief of MI (OCMI), the International Military Student Office, the University of Military Intelligence, the Military Intelligence Online Library, Lessons Learned, and other informative sites. I challenge you to visit the ICON site to become familiar with the products available and to share your lessons learned comments.

Critical Task Site Selection Boards

The Critical Task Site Selection Board (CTSSB) is the vehicle we use to keep training current and relevant with the ever changing missions of our highly technical MI Military Occupational Specialties (MOSs). Critical tasks are adjusted as a result of recommendations made by the CTSSBs, which in turn cause changes to MOSs. It is very important to have as many units as possible participate in the CTSSBs to ensure that new tasks are captured and tasks that are no longer required are deleted to focus limited training resources on the tasks and skills our Soldiers need today and tomorrow. It is critical that you send your sharpest and brightest. Here is a list of scheduled full CTSSBs; those scheduled more than six months out are subject to change. You can check for any changes to the CTSSB schedule on Army Knowledge Online (AKO).

MOS	Date	Location
98C/352N	01-12 May 2006	Goodfellow AFB, TX
33W/353T	07-18 Aug 2006	Fort Huachuca, AZ
98Y/352S	16-27 Oct 2006	Fort Huachuca, AZ
97E/351L	Fall 2006	Fort Huachuca, AZ
97B/351L/35E	April 2007	Fort Huachuca, AZ
35C/35D/35G	Oct 2007	Fort Huachuca, AZ
96D/350G	Dec 2007	Fort Huachuca, AZ

(Continued on page 5)

when we deployed to Iraq the country brief was pretty much handed to us. —Sergeant, S2 NCOIC, Engineer Group

From El Salvador to Iraq, the U.S. Army operates in diverse operational environments around the world. These diverse operational environments mean the development and use of open source intelligence is not a luxury but a necessity. Open sources possess much of the information that we need to understand the physical and human factors of the operational environments in which we conduct or may conduct military operations. In truth, much of our understanding of these environments is based on publicly available information obtained through educators, journalists, news anchors, and scholars. We believe this concept is captured within the following characteristics of OSINT:

- **Provides the Foundation.** Publicly available information forms the basis of all intelligence operations and intelligence products.
- **Answers Requirements.** The availability, depth, and range of public information enables intelligence organizations to satisfy many intelligence requirements without the use of specialized human or technical means of collection.
- **Enhances Collection and Production.** OSINT operations support other ISR efforts by providing information that enhances collection and production.
- **Benefits Multidiscipline Intelligence.** As part of a multidiscipline intelligence effort, the use and integration of OSINT ensures decisionmakers have the benefit of all-sources of available information.

The U.S. Army Intelligence and Security Command's Asian Studies Detachment (ASD) demonstrates these characteristics and the power of sustained OSINT operations. Since 1947, ASD has collected, processed, and analyzed publicly available information on the capabilities, disposition, and readiness of the military forces of China, North Korea, and other potential adversaries. It has also reported on the economic, environmental, political, and social conditions within the region. In recent years, ASD reported on—

- Elevated tensions between China and Taiwan during the Taiwan presidential elections in 2004.
- Security threats to U.S and allied forces conducting humanitarian relief operations in Indonesia following the December 2004 tsunami devastation
- Strategy and tactics employed during the August 2005 Sino-Russian combining counterterrorism Exercise PEACE MISSION 2005.

As testimony to the high value of OSINT analysis and reporting, ASD's intelligence information reports since 2003 have received 28 "Major Significance" evaluations from the Defense Intelligence Agency, National Ground Intelligence Center, and the U.S. Air Force's National Air and Space Intelligence Center on topics ranging from North Korean underground facilities to Chinese Peoples Liberation Army Air Force air and space science and technology developments.

FMI 2-22.9 serves as a catalyst for discussing and defining Army OSINT. During its two-year lifecycle, the TTPs in this manual will evolve as the Army and the Intelligence Community (IC) work to integrate and synchronize OSINT operations between echelons. This evolution will occur, in part, as the Director of National Intelligence (DNI) Open Source Center undertakes the difficult task of "coordinating the collection, analysis, production, and dissemination of open source intelligence to elements of the IC" in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004. In the end, the Army and the IC will reach consensus about the "who, what, where, when, why, and how" of OSINT operations. This consensus will take form in future Army and Joint intelligence doctrinal literature as well as Director of National Intelligence guidance and the DNI Open Source Center's synthesis of IC's OSINT best practices.

American military professionals have used publicly available information in order to produce intelligence throughout our history. The value of publicly available information as a source of intelligence has, however, often been overlooked in American intelligence operations. However, USAIC&FH is moving out to improve intelligence operations by addressing OSINT across doctrine, organizational structures, training, materiel, and leadership development. The establishment of OSINT as an Army intelligence discipline is an important first step toward ensuring that we, the Army's Military Intelligence professionals, provide decisionmakers with actionable intelligence derived from all sources of information.

ALWAYS OUT FRONT!

CSM Forum (Continued from page 3)

Changes in MI MOSs

It is important for the Soldiers within your organizations to understand the changes affecting the MI Corps. OCMI provides update briefs for the officer, warrant officer (WO) and noncommissioned officer (NCO) training courses conducted at Fort Huachuca. OCMI is also available to provide Officer Professional Development (OPD) and NCOPD for organizations. An abbreviated version of the information these briefs provide follows.

MOS Recoding

Headquarters, Department of the Army (HQDA) directed the recoding of MOSs across the force to align Career Management Fields (CMFs). The MI WO MOSs was recoded 30 September 2005.

MOS 350 Military Intelligence	MOS 352 Signals Intelligence/Electronic Warfare (IEW)
350B (350F) All Source Analysis Technician	352C (352N) Traffic Analysis Technician
350D (350G) Imagery Intelligence Technician	352G (352P) Voice Intercept Technician
350L (350Z) Attache Technician	352H (352Q) Communications Interceptor/ Technician
350U (350K) Tactical Unmanned Aerial Vehicle (TUAV) Operations Technician	352J (352R) Emanations Analysis Technician
MOS 351 Human Intelligence (HUMINT)	352K (352S) Non-Morse Intercept Technician
351B (351L) Counterintelligence Technician	MOS 353 Intelligence and Electronic Warfare
351C (351Y) Area Intelligence Technician	353A (353T) IEW Systems Maintenance Technician
351E (351M) Human Intelligence Collection	

CMF 96, 98, and 33 will be recoded to CMF 35 effective 30 September 2007. Coding of the officer areas of concentration (AOCs) will not change.

CMF 96 Military Intelligence	CMF 98 Signals Intelligence/Electronic Warfare Operations
96B (35F) Intelligence Analyst	98C (35N) Signals Intelligence Analyst
96D (35G) Imagery Analyst	98G (35P) Cryptologic Linguist Interceptor/ Locator
96H (35H) Common Ground Station Operator	98Y (35S) Signals Collector/Analyst
96Z (35X) Intelligence Senior Sergeant	98Z (35Z) Signals Intelligence (SIGINT) Senior Sergeant
97B (35L) Counterintelligence (CI) Agent	CMF 33 MI Systems Maintenance and Integration
97E (35M) Human Intelligence (HUMINT) Collector	33W (35T) MI Systems Maintainer/Integrator
97Z (35Y) CI HUMINT Senior Sergeant	

Specific MOS Changes

CMF 33.

Approximately 212 MOS 33W (35T) UAV coded positions are projected to convert to the aviation MOS 15J, **OH-58D Armament/Electrical/Avionics Systems Repairer** effective Fiscal Year (FY) 09. The 33W Soldiers currently filling those positions will not reclassify unless they request to do so. Soldiers currently qualified in MOS 15J will attend UAV training incrementally to replace MOS 33W in UAV units.

CMF 96.

Requirements are projected to increase for most of CMF 96 during the transformation to the Modular Force. MOS 96B increases from 4088 to 5652, MOS 96D decreases from 820 to 796, and MOS 96H increases from 694 to 738. A big concern for MOS 96D and 96H career progression is the decrease in Master Sergeant (MSG) positions from 27 to 12. Based on this decrease and recommendations from Sergeants Major across the force, OCMI recommended capping MOS 96Z at MSG versus the Sergeant Major (SGM) level. The Commanding General, USAIC&FH approved this recommendation in the FY06 Military Occupational Classification and Structure (MOCS) proposal. If approved by HQDA, this will result in a better distribution of MSG slots for the entire CMF 96. OCMI has requested early implementation of this action to occur before FY09.

MOS 96B and 96D remain on the STAR MOS list for both Sergeant (SGT) and Staff Sergeant (SSG). Major General Fast and I need every leader to take a hard look at your formations and make sure all eligible Soldiers in STAR MOSs are counseled properly, if they are not recommended for promotion. Sixteen eligible 96B and 96D Soldiers were selected for DA Directed Automatic List Integration (DALI) to SGT for January 2006. The DALI was established by DA to help fix NCO shortage issues within STAR MOSs. Soldiers in the primary zone and eligible for promotion (but not recommended) can now be DA-selected for promotion with 350 promotion points.

The FY05 CTSSB for MOSs 96D and 96H recommended some changes that bring the skill sets of these two MOS closer together. The Imagery Intelligence (IMINT) “Cradle to Grave” Study is scheduled to begin March 2006 to evaluate every aspect of IMINT, similar to the recently conducted Signals Intelligence (SIGINT) “Cradle to Grave” Study. During this study the possibility of merging MOSs 96D and 96H will be reviewed. Of note, the 96D FY05 CTSSB, held 5 to 16 December 2005, added nine Skill Level (SL) 1 tasks emphasizing Moving Target Indicator (MTI), (traditionally an MOS 96H function), the All-source Analysis System (ASAS), and Distributed Common Ground Station (DCGS)-A Operations. Five additional tasks were added to SLs 3 and 4 which emphasize higher imagery analysis skills and management. The MOS 96H FY05 CTSSB, held 15 to 19 August 2005, added a TOP SECRET (TS) clearance requirement to this MOS; changed the duty title from Operator to Analyst; added 15 new tasks emphasizing the Joint Tactical Terminal (JTT), MTI Forensics, and UAV Remote Video Terminal (RVT).

Effective 1 October 2006 MOS 96R, Ground Surveillance System Operator, is deleted from the Active Component. While it is preferable that MOS 96R Soldiers reclassify into another MI MOS, it may not be possible for all to do so. In order to avoid mandatory reclassification based on needs of the Army, MOS 96R Soldiers need a projected class seat prior to July 2006, although the actual class may not start until after October 2006. OCMI continues to work waiver issues with the Human Resources Command (HRC) for MOS 96R Soldiers who wish to remain MI but are lacking prerequisites.

MOS 96U transitions to the Aviation Branch Proponency by FY08 and will become MOS 15W.

Effective 1 October 2006, MOS 97B will no longer be an entry-level MOS and all current 97B10 positions will be recoded to 97E10. MOS 97B will begin at the rank of SGT, creating a significant in-service recruiting requirement. MOS 97E is the MOS of choice for in-service recruiting for MOS 97B applicants, but MOS 97E

Soldiers who choose to re-classify into MOS 97B are still required to go through the full MOS 97B (CI Applicant) process. MOS 97B requirements decrease from 1645 to 1305 during transformation to the Modular Force. MOS 97E requirements increase from 967 to 3330. MOS 97B remains on the STAR MOS list for SSG and 97E remains on the STAR MOS list for SGT and SSG. An additional MOS 97B issue being worked between OCMI, HRC, and HQDA G1 are the MOS 97B10 Soldiers who are currently in the force. Per the Notification of Future Change (NOFC) 0404-27, MOS 97B10 Soldiers can serve in MOS 97E10 positions thru FY09. By the end of FY09 most, if not all MOS 97B10 Soldiers, will either be promoted to MOS 97B20 or will have left the Army. Therefore, there is no immediate need to reclassify the MOS 97B10 Soldiers in the force. Implementation clarification is currently at HQDA G1 for comment. Updates related to this particular issue will be addressed in the future.

On 19 December 2005, the CG, USAIC&FH, briefed the Deputy Chief of Staff, G2 and the CG, U.S. Army Intelligence and Security Command (INSCOM) concerning MOS 97E. The briefing outlined the results and recommendations from an MOS review conducted by USAIC&FH with USAIC&FH as the lead, and HQDA, HRC. and U.S Army Training and Doctrine Command (TRADOC) in support. A complete evaluation of MOSs 97E and 97B Force Structures and Standard of Grade (SOG) are being conducted by Directorate of Combat Developments (DCD). If approved by DA, the following changes are expected by Spring 2006:

- A temporary suspension of the language requirement for promotion eligibility for all MOS 97E Soldiers at all grades. This suspension will be re-evaluated annually. Soldiers awarded MOS 97E during the suspension period are considered “grandfathered” and will not require a language for the duration of their career. However, they will be allowed to attend language training if they request to do so.
- Only a limited number of MOS 97E Soldiers will reclassify to MOS 97B until the MOS 97E strength is at or near 90 percent.
- The maximum selective reenlistment bonus (SRB) will increase from $20K to $40K, and the Critical Skills Retention Bonus (CSRB) will increase to a maximum of $150K with a 6-year extension for retirement eligible Sergeants First Class (SFC) and MSGs, regardless of their retention control point (RCP).

CMF 98.

CMF 98 went through a major transformation on 1 October 2005. First, MOS 98C absorbed the Operational Electronic Intelligence (OPELINT) skill sets from MOS 98J. Soldiers formerly qualified in either of these MOSs must attend transition training in order to become MOS qualified as a “new” 98C. MOS 98C requirements increase during transformation to the Modular Force from 2094 to 3177. Second, MOS 98Y was formed by merging 98J and 98K. MOS 98Y absorbed the Technical Electronic Intelligence (TECHELINT) skill sets from MOS 98J. Soldiers formerly qualified in either of these MOS must attend transition training in order to become MOS 98Y qualified. MOS 98Y requirements will increase during transformation to the Modular Force from 905 to 1042.

MOS 98H merged into MOS 98G and identified by Skill Qualification Identifier (SQI) A, meaning Morse vice a language. Subsequently, INSCOM requested that 98GA positions be recoded to MOS 98Y. MOS 98GA will be deleted effective 1 October 2006, requiring Soldiers in MOS 98GA to reclassify. Please have your 98GA Soldiers work with their retention NCOs and HRC to reclassify into a new MOS as soon as possible. It is our goal to maintain as many 98GAs in the MI community as possible.

Current Status of Transition Training Funding. Though MTSA funding for the four CMF 98 transition training courses may now be used for this training, units are still being asked to pay for some of their Soldier’s training out of operational budgets. This is because 30 percent of the class seats have been coded in the Army Training Requirements and Resources System (ATRRS) as MTSA funded with temporary duty (TDY) enroute

and in conjunction with a permanent change of station (PCS). The other 70 percent are coded TDY and return to duty station which are paid for by the unit. We have not yet filled the 30 percent of the MTSA funded class seats in ATRRS. If any unit wants to send a Soldier to training in a TDY and return status, but does not have sufficient training funds to do so, HQDA G3 has asked to be notified (through HRC MI Branch) immediately. Additionally, Fort Huachuca is currently cross-walking an INSCOM proposal of using alternate National Cryptologic School (NCS) courses to meet the transition qualification requirements. This may also provide another avenue for Soldiers to be trained. Note: The resident transition courses are programmed to be available for FY06-FY11.

Scheduled Class Dates

MOS 98C to 98C (Fort Huachuca, AZ)

Start dates:

TY06: 10 April, 8 May, 5 June, 10 July, 31 July, 28 August, 25 September,16 October, 13 Nov,

TY07: 8 January, 5 February, 5 March, 2 April, 30 April, 21 May, 18 June, 16 July, 6 August, 10 September

MOS 98K to 98Y (Fort Huachuca, AZ)

Start dates:

TY06: 30 May, 19 June, 24 July, 21 August, 16 October,

TY07: 8 January, 5 March, 30 April, 25 June, 20 August

MOS 98J to 98C (Goodfellow Air Force Base, TX)

Start dates:

TY06: 3 May, 2 August,

TY07: 26 January, 27 April, 27 July

MOS98J to 98Y (Pensacola, FL)

Start dates:

TY06: 17 April, 1 May, 15 May, 30 May, 5 June, 19 June, 3 July, 17 July, 31 July, 7 August, 21 August, 5 September, 18 September,

TY07: 16 January, 22 January, 5 February, 12 February, 26 February, 19 March, 26 March, 9 April, 30 April, 21 May, 29 May, 11 June, 2 July, 23 July, 13 August, 20 August, 4 September, 24 September.

MOS 09L. The MI Corps is working to establish a new Active Duty MOS 09L (Interpreter/Translator). Analysis on proposed structure and lifecycle is ongoing. A Table of Distribution and Allowances (TDA) with 104 positions has been established. This MOS is planned to have a full lifecycle from E3–E9.

Combat Tracking Course

USAIC&FH recently established a Combat Tracking Course to prepare Soldiers and law enforcement personnel (Homeland Defense) for combat and tactical tracking operations against insurgents and criminal elements; provide training in gathering forensic evidence tying criminals and/or enemy forces to incidents; and educate students in the fundamentals of tracking human subjects in varying terrain and weather conditions to generate targetable intelligence. This course ties to “Every Soldier is a Sensor” concept. The Basic Tracking

Course is 5 days; the expanded course is 10 days. The website, at http: www.universityofmilitaryintelligence.us/homeland/ctc/default.asp, gives examples of the intelligence value gained from the course. If you have questions about the course, contact COL Stephanie Hap at (520) 533-9496 DSN 821-9496. This is not, and will not be, a Mobile Training Team. Fort Huachuca ***can*** replicate the appropriate training environments.

Conclusion

The MI Corps is undergoing many changes in our enlisted MOSs at this time and it is important for all Soldiers to stay informed. I will continue to distribute updates through the CSMs and SGMs via email. I am extremely proud of our Intelligence Warriors and the contributions you make each day to support our Nation at War!

SOLDIERS ARE OUR CREDENTIALS

Managing Army Open Source Activities

by Craig Manley

The effective use of open sources and exploitation of open source (OS) information has appropriately received renewed emphasis from advocates of OS and in authoritative documents such as the *9/11 Commission Report* and the *Intelligence Reform and Terrorism Prevention Act*. [1] Various recommendations concerning OS activities were proffered but lacking an enterprise-wide assessment it was difficult to evaluate these recommendations. The Office of the Under Secretary of Defense for Intelligence (OUSD(I)) decided to form a working group to conduct an enterprise-wide assessment. The Department of the Army (DA) G-2 staff participated in this assessment.

By the fall of 2004 the working group had completed an initial report which stated that OS *policy and doctrine* were inadequate; *training* was neither standardized nor defined; *management* of OS activities lacked a defined construct and process; and that Department of Defense (DOD) OS *requirements* were under represented and under funded within the Intelligence Community (IC).

The report stimulated the establishment of the Defense Open Source Council (DOSC). The DOSC was chartered by the USD(I) to broaden the initial assessment, propose operational improvements across the enterprise, and establish implementing plans. The near-term tasks for the council were to—

- ❑ Develop a comprehensive understanding of OS requirements.
- ❑ Develop an OS intelligence strategy for the DOD.
- ❑ Develop an investment strategy.
- ❑ Recommend a management construct.
- ❑ Facilitate the development of OS policy and doctrine.
- ❑ Increase DOD participation in IC level OS forums.

Several Army OS activities provided examples of mature and highly effective benchmarks, including U.S. Army Intelligence and Security Command (INSCOM) MI Battalion-Japan, the Asian Studies Detachment (ASD), the National Ground Intelligence Center (NGIC) Information Management Division, and TRADOC's Foreign Military Studies Office (FMSO). The intelligence research skills training conducted by staff at the Military Intelligence (MI) Library at the U. S. Army Intelligence Center and Fort Huachuca (USAIC&FH) and the OS activities of the 902d MI Group's Army Counter Intelligence Center (ACIC) also provided exemplars for others to emulate.

Additional pockets of individual expertise and organizational richness came to light during the April 2005 Army OS Practitioners meeting held at the NGIC. The meeting initiated a series of conferences to bring together Army OS practitioners to discuss and identify improvements to requirements management, vendor contracting, automation support techniques, and research skills.

USAIC&FH has moved out aggressively to write an interim Field Manual (FMI) for OS intelligence. The

discussion at the April meeting set the baseline for much of the content of what has become **FMI 2-22.9, Open Source Intelligence**. The manual will be the first Service level text on the subject and will set a standard for doctrinal and training improvement efforts within the DOD.

By the time this article is published, another meeting of the Army OS community will have been held at Fort Leavenworth. That meeting and subsequent meetings will draw on what is needed to respond to intelligence requirements, to share lessons learned, and to determine the additional tools and resources needed to continue improving the OS Intelligence (OSINT) discipline.

The role of the Army G2 OS Functional Coordinator is to identify and assist in closing gaps in capabilities, processes, organizations, and resources within the Defense and National ICs. We focus on training needs and resources, access to content, tools, and management processes. We participate in working groups to characterize and develop solutions to issues of common concern. *Our bottom line*: Ensure the Army OS and all-source ICs reap the benefits of economical but valuable OS information content, state of the art analytics tools, and effective policy and doctrine.

Endnotes

1. References to the use of Open Source information can be found in the *9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition* on pages 411 and 413 and in the *Intelligence Reform and Terrorism Prevention Act of 2004* in Section 1052 on page 47. Both documents are available without cost at *www.gpoaccess.gov.*

Craig Manley serves in Headquarters, DA, Office of the Deputy Chief of Staff, G2 as an intelligence specialist in Intelligence Production Functional Management. He is concurrently the DA G2 Functional Coordinator for OSINT. Mr. Manley retired from the U.S. Army as Command Sergeant Major, 704th Military Intelligence Brigade, in November of 1996. He joined the G2 as a program analyst for the National Foreign Intelligence Program in the Resource and Integration Directorate in 2000. Mr. Manley is certified as an IC Officer in several disciplines. He holds a Master's Certificate in Government Contracting from George Washington University and a Bachelor's Degree in Asian Studies from the University of Maryland. He can be reached at Francis.Manley@us.army.mil or (703) 695-1636.

The Government Printing Office (GPO) has authorized MIPB to sell back issues for $2.50 each. If you wish to purchase issues, email your request to **MIPB@hua.army.mil**. Tell us the issue(s) you want (e.g., January-March 2002) and how many.

Doctrine Corner

Open Source Intelligence Doctrine

by Michael C. Taylor

FMI 2-22.9, Open Source Intelligence, provides interim tactics, techniques, and procedures (TTPs) for open source intelligence (OSINT) operations. It provides a basic description of the fundamentals of OSINT, the planning of OSINT operations and support; the collection and processing of publicly available information; and the production of OSINT. As interim doctrine, FMI 2-22.9 provides not just basic techniques and procedures but serves as a catalyst for increasing awareness of OSINT and improving Army OSINT operations. This article presents the fundamentals of OSINT operations found in this emerging intelligence doctrine, FMI 2-22.9.

What is OSINT?

OSINT is relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to intelligence requirements. Two important terms in this definition are–

- **Open Source.** Any person, group, or system that provides information without the expectation that the information, relationship, or both, are protected against public disclosure.
- **Publicly Available Information.** Data, facts, instructions, or other material published or broadcast for general public consumption available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

The OSINT Discipline

OSINT operations are integral to Army intelligence operations. Publicly available information forms the basis of all intelligence operations and intelligence products. The availability, depth, and range of publicly available information enable intelligence organizations to satisfy many intelligence requirements without the use of specialized human or technical means of collection. OSINT operations support other intelligence, surveillance, and reconnaissance (ISR) efforts by providing information that enhances collection and production. As part of a multidiscipline intelligence effort, the use and integration of OSINT ensures decisionmakers have the benefit of all available information.

The source and the collection means rather than a specific category of technical or human resources distinguish OSINT from other intelligence disciplines. Open sources broadcast, publish, or otherwise distribute information for public use. The collection means (techniques) for gathering publicly available information from these media of communications are overt and unintrusive. Other intelligence disciplines use covert or intrusive techniques to collect private information from confidential sources.

Open Source Media

Communications consist of a sender, a message, a medium, and a receiver. The medium is the access point to publicly available information for open source research and collection. The primary media that open sources use to communicate information to the general public are—

- **Public Speaking Forums.** Public speaking, the oldest medium, is the oral distribution of information to audiences during events that are open to the public or occur in public areas. These events or forums include but are not limited to academic debates, educational lectures, news conferences, political rallies, public government meetings, religious sermons, and science and technology exhibitions. Neither the speaker nor the audience has the expectation of privacy when participating in a public speaking forum. Unlike the other open source collection, monitoring public speaking events is done through direct observation and, due to its overt nature, could entail risk to the collector.

- **Public Documents.** A document is any recorded information regardless of its physical form or characteristics. Like public speaking, public documents have always been a source of intelligence. Documents provide in-depth information about the operational environment (OE) that underpin our ability to plan, prepare for, and execute military operations. During operations, documents such as newspapers and magazines provide insights into the effectiveness of information operations. Books, leaflets, magazines, maps, manuals, marketing brochures, newspapers, photographs, public property records, and other forms of recorded information continue to yield information of intelligence value about operational environments. Sustained document collection contributes to the development of studies about potential OEs. Document collection on the operational and technical characteristics of foreign materiel aids in the development of improved U.S. tactics, countermeasures, and equipment.
- **Public Broadcasts.** A public broadcast entails the simultaneous transmission of data or information for general public consumption to all receivers or terminals within a computer, radio, or television network. Public broadcasts are important sources of current information about the OE. Television news broadcasts often provide the first indications and warning (I&W) of situations that may require the use of U.S. forces. Broadcast news and announcements enable personnel to monitor conditions and take appropriate action when conditions change within the area of operations. News, commentary, and analysis on radio and television also provide windows into how governments, civilians, news organizations, and other elements of society perceive the U.S. and U.S. military operations. Broadcasts also provide information and insights into the effectiveness of information operations both lethal and non-lethal.
- **Internet Sites.** Internet sites enable users to participate in a publicly accessible communications network that connects computers, computer networks, and organizational computer facilities around the world. The Internet is more than just a research tool. It is a reconnaissance and surveillance tool that enables intelligence personnel to locate and observe open sources of information. Through the Internet, trained collectors can detect and monitor Internet sites that may provide I&W of enemy intentions, capabilities, and activities. Collectors can monitor newspaper, radio, and television websites that support assessments of information operations. Collectors can conduct periodic searches of web pages and databases for content on military order of battle, personalities, and equipment. Collecting web page content and links can provide useful information about relationships between individuals and organizations. Properly focused, collecting and processing publicly available information from Internet sites can help analysts and decision makers understand the operational environment.

OSINT Considerations

For the most part, the considerations for OSINT are similar to those of other intelligence disciplines. OSINT organizations need clearly stated intelligence requirements to effectively focus collection and production. OSINT operations must comply with **Army Regulation 381-10, U.S. Army Intelligence Activities,** and **Executive Order 12333, U.S Intelligence Activities,** on the collection, retention, and dissemination information on U.S. persons. OSINT organizations can be overwhelmed by the volume of information to process and analyze. OSINT operations require qualified linguists to collect and process non-English language information. In addition to these common considerations, personnel responsible for planning or executing OSINT operations must consider the following:

- **Limitations.** Intelligence organizations whose principal missions are counterintelligence, human intelligence, and signals intelligence must comply with applicable Department of Defense Directives and Army Regulations that govern contact with and collection of information from open sources. For example, Department of Defense Directive 5100.20 prohibits signals intelligence organizations from collecting and processing information from public broadcasts with exception of processing encrypted or “hidden meaning” passages.
- **Operations Security.** More than any other intelligence discipline, the OSINT discipline could unintentionally provide indicators of U.S. military operations. Information generally available to the public as well as certain detectable activities such as open source research and collection can reveal the existence of, and sometimes details about, classified or sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit US military operations. Purchasing documents, searching an Internet site, or asking questions at public events are examples of detectable open source research and collection techniques that could provide indicators of U.S.

plans and operations. Using the five-step operations security process, organizations must determine what level of contact with open sources and which collection techniques might provide indicators that an enemy could piece together in time to affect U.S. military operations. The steps of the process are identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures. In OSINT operations, countermeasures range from limiting the frequency or duration of contact with a source to prohibiting all contact with a source.

- **Deconfliction.** During planning, the G2/S2 staff and the G3/S3 staff must deconflict ISR operations. Specifically, collection may compromise the operations of another intelligence discipline. Contact or interaction with open sources may adversely affect the ability of non-intelligence organizations such as civil affairs, military police, medical, and public affairs to accomplish their missions. Overt contact with a source by civil affairs, military police, or other personnel may compromise OSINT operations as well as the safety of the open source or collector. Each of these situations could lead to the loss of access to the open source and information of intelligence value.
- **Deception and Bias.** Deception and bias are of particular concern in OSINT operations. Unlike other disciplines, these operations do not normally collect information by direct observation of activities and conditions within the area of interest. OSINT operations rely on secondary sources to collect and distribute information that the sources may not have observed themselves. Secondary sources such as government press offices, commercial news organizations, nongovernmental organization spokesmen, and other information providers can intentionally or unintentionally add, delete, modify, or otherwise filter the information they make available to the general public. These sources may also convey one message in English for U.S. or international consumption and a different non-English message for local or regional consumption. It is very important to know the background of open sources and the purpose of the public information in order to distinguish objective, factual information from information that lacks merit, contains bias, or is part of an effort to deceive the reader.
- **Intellectual Property. Army Regulation 27-60, Intellectual Property,** prescribes policy and procedures with regard to the acquisition, protection, transfer and use of patents, copyrights, trademarks, and other intellectual property by the Department of the Army. It is Army policy to recognize the rights of copyright owners consistent with the Army's unique mission and worldwide commitments. As a general rule, Army organizations will not reproduce or distribute copyrighted works without the permission of the copyright owner unless such use is within an exception under U.S. Copyright Law or required to meet an immediate, mission-essential need for which non-infringing alternatives are either unavailable or unsatisfactory. According to the U.S. Copyright Office, "fair use" of a copyrighted work for purposes such as criticism, comment, news reporting, teaching, scholarship, or research, is not an infringement of copyright.

Conclusion

FMI 2-22.9 is scheduled for publication during the summer of 2006. As with any field manual, its measure of effectiveness will be demonstrated in how well the TTPs enable users to accomplish their missions. Hopefully, the manual will be successful since failure means commanders and their soldiers may not be benefiting from one of the most abundant sources of information on the OE. It is incumbent upon you, the initial users of FMI 2-22.9, to put the doctrine through its paces and send your feedback to the Intelligence Center. Your feedback will improve not just the doctrine but the training and the tools that enable effective OSINT operations.

Michael Taylor is a senior intelligence analyst for ARSC Communications. He is currently the OSINT Doctrine Project Leader for the Directorate of Doctrine of the U.S. Army Intelligence Center at Fort Huachuca, Arizona. His background includes 25 years of military and civilian experience in National, operational, and tactical intelligence operations, primarily as an intelligence analyst and Russian linguist. Mr. Taylor's previous doctrinal literature works include: **FM 34-1, *Intelligence Operation*; FM 34-25-3, *All-Source Analysis System and the Analysis and Control Element***; *three Special Texts on Objective Force division and brigade intelligence operations; a series of studies on the doctrinal implications of the Distributed Common Ground System-Army; and several articles in the* ***Military Intelligence Professional Bulletin***.

DOD and the DNI Open Source Center–

Building the Partnership

Editor's Note: There are four articles from the DNI Open Source Center in this issue of MIPB. Two of the articles, DOD and the DNI Open Source Center–Building the Partnership and The Open Source Academy Helps the Intelligence Community Make the Most of Open Sources, are unclassified. The other two articles, History of Open Source Exploitation in the Intelligence Community and OpenSource.gov, are FOUO and can be found on the sensitive but unclassified (SBU) "side" of MIPB. Request a user's account to read these and other articles at the MIPB Home Page, http://www.umi-online.us/mipb. For more information on the Open Source Center, call Customer Service at 1.800.205.8615.

by Douglas Peak

Growing Outreach to the Combatant Commands

Department of Defense (DOD) components represent the largest segment of the Director, National Intelligence (DNI) Open Source Center's (OSC) customer base, and many of its organizations have long-standing relationships with the Center and its predecessor, the Foreign Broadcast Information Service (FBIS). Strengthening and expanding those partnerships and the level of collaboration is a keystone of the Center's strategic objectives. The partnership with the nine Combatant Commands (COCOMs) is especially important because of their broad and direct role in the Global War on Terrorism (GWOT) and because of the many significant OS activities resident in some of the commands. Over the last year, the OSC has taken a number of steps to build on what was already a solid working relationship. The goal has been to more closely engage the commands to form mutually beneficial relationships in exploiting OS and carrying out media analysis in support of the warfighters' mission.

A First-Ever Meeting

Most notable among the growing contacts between the Center and the commands was the first-ever FBIS-DOD Under secretary of Defense for Intelligence (USD(I)) Conference, held outside Washington D.C. in July 2005. The jointly sponsored conference focused on developing strategies and recommendations for facilitating closer and more effective OS support to the COCOMs and the National Guard. More specifically, the conference was intended to provide a forum that would facilitate the sharing of information on OS collection, analysis, and dissemination, and the identification of opportunities for collaboration between the then FBIS and the COCOMs. It was the first time that the OSC had met with all the Commands together. The meeting also provided an opportunity for the various OS units to connect.

Nearly 100 participants, about evenly divided between DOD and the OSC, attended the three-day conference. On the DOD side, in addition to participants from the Commands and the National Guard, attendees included the Defense Intelligence Agency (DIA) and the other key combat support agencies, as well as the National Virtual Translation Center (NVTC), which is housed in the Federal Bureau of Investigation (FBI) but provides extensive support to the COCOMs. Program managers, key project managers, and subject-matter experts from the OSC participated and provided insights into the Center's collection and analytical capabilities. The conference attracted considerable high-level attention within the Intelligence Community (IC) because of the growing recognition of the important role of OS in support of military operations.

The first day of the conference was built around a series of presentations by the OSC, the COCOMs, and the National Guard, creating a baseline understanding of coverage responsibilities, capabilities, and challenges. These presentations set the stage for the working groups that focused on key issues raised by the commands:

- ❑ Managing OSINT requirements.
- ❑ Information sharing and dissemination.
- ❑ Leveraging subject-matter experts.
- ❑ Technology enablers.

The second and third days centered on work in four smaller break-out sessions, ending with presentations that included recommendations for moving forward

in the four key issue areas. Several themes became quickly apparent as the groups came back together to present their findings. On the positive side:

- ❑ OS has emerged as an important source of intelligence from the bottom up, rather than being driven from the top down.
- ❑ OS provides alert functions and is often the only reporting available to respond to requests.
- ❑ The demand for OS support will continue to grow very quickly.

At the same time, however, virtually all of the commands and the National Guard face common challenges in meeting OS requirements, most notably:

- ❑ Unclassified information does not compete well against classified information—a culture of "If it's unclassified, it must not have value" still pervades the IC.
- ❑ OS collection is poorly funded and units are understaffed.
- ❑ The lack of access to the Internet at the desktop is a huge obstacle to OS collection and analysis.
- ❑ Defense OS cells have no training in media analysis and lack language capabilities.
- ❑ There is no clear external point of contact or central responsibility for OS support for the military.
- ❑ Legal interpretation of the use of publicly available (i.e, open) sources is varied and inconsistent.
- ❑ Access to OS research tools is limited or even nonexistent.

Conference participants worked to develop a common understanding of these challenges and to formulate some strategies and recommendations to address them in the near and long term. Participants flowed through the four key interest area sessions, first defining the issues, then developing strategies and possible "quick wins," as well as potential "red flags." On the last morning the original groups met again and developed recommendations and quick wins that were then briefed and discussed by all the attendees.

By all accounts the conference was a success, marking a strong start toward building a long-term productive, mutually beneficial relationship. The OSC plans to hold a community-wide conference within a year to build on and expand the work of this first joint OSC-DOD OS conference.

Supporting the Information Operations Mission

Information Operations (IO) dovetail tightly into the mission of the OSC, and the Center already plays a role in the command's Strategic Communications initiative. The OSC is well positioned to broaden support to the command's multi-faceted IO mission at several key points through—

- ❑ Media surveys that can help identify how key demographic groups obtain news and generally stay informed.
- ❑ Tailored coverage that can help gauge public and official reaction to the Commands' theater engagement activities in their respective areas of responsibility (AORs) as well as other U.S. diplomatic and economic relationships in the regions.
- ❑ Collection of gray literature, which can provide a good sense of public opinion on a local level.

The Ongoing Partnerships as Forerunners

Strong ties that exist now between the COCOMs and the OSC illustrate the potential for the growing partnerships in the following areas.

Geospatial Information

The unique service provided by the OSC and its predecessor organizations, especially the skills and knowledge of what type of mapping and geographic information is openly available and how to apply it, has drawn the attention of military services for more than 60 years. Fully 25 percent of the geospatial information disseminated by the OSC goes to the military, ranging from the COCOMs to individual small units. The military has called on OSC's expertise for operations from noncombatant evacuations in the wars in Africa to combat operations in the Balkans, Afghanistan, and Iraq.

Working with the Surface Deployment and Distribution Command (SDDC), the OSC obtained road and navigation data to assist in contingency planning for rescue and reconstruction efforts for natural disasters and humanitarian relief efforts for India, Korea, and other countries. Such information as road surfaces, bridge types, harbor depths, and port facilities allow the SDDC to plan sea and land routes for heavy equipment and personnel to heavily popu-

lated as well as out-of-the-way locations in the event of an emergency.

Commands and service components frequently turn to the OSC as a source of commercial and foreign mapping to augment what is available from other government agencies. In advance of Operation ENDURING FREEDOM, Special Operations Command used OSC-provided data to plan operations and set up bases. In Iraq, DOD units turned to the OSC to obtain useful and openly available information detailing addresses and ownership of buildings and other property. The OSC converted the information into digital maps that was then incorporated into "MapQuest™"-like products allowing service personnel to narrow down coordinates to within a house of a desired location as opposed to within a neighborhood. That ability minimizes collateral damage in the event of firefights as well as the time troops have to spend in potentially hostile environments. Prior to this effort, units had to sift through mounds of paper in order to find a neighborhood or a street address. Whereas previously, hours were spent to find a location, finding locations in cities for which address data is available now takes minutes.

Collection and Product Support

A striking example of DOD-OSC cooperation takes place in the Pacific Command (PACOM) AOR where the 500th Military Intelligence Brigade's Asian Studies Detachment (ASD) at Camp Zama (See David Reese's article on the ASD in this issue of ***MIPB***) has created links with an OSC Bureau in Asia and the OS Academy at OSC headquarters. Coordination between ASD and the OSC resulted in the OSC taking on the daily headline summary of the on-line version of the leading Chinese military newspaper, freeing up an ASD resources to focus on other important mission tasks. ASD makes its monthly acquisitions list available to OSC analysts and provides copies of requested materials, expanding the amount of OS data available from the region for OSC to exploit, saving resources by reducing redundant collection. Consistent with the community's broad goal of increasing product availability, OSC is rehosting ASD's Force Protection and Situational Awareness Report, posting it on OSC's unclassified, Internet-based dissemination platform—OpenSource.gov. (See Douglas Peak's article on OpenSource.gov in this issue.) Finally, ASD has taken advantage of OSC's drive to support OS training across the government by sending two senior managers to participate in core courses at its OS Academy.

Acquisition of Open Source Material

The OS Acquisition Center (OSAC), a branch of the OSC library, supports several military installations by supplying them with foreign publications ordered from U.S. embassies and OSC bureaus around the world. OSAC supplies customers with a variety of military, government, political, and economic publications as well as a cross section of newspapers. Several military customers, including the Defense Language Institute, have a heavy need for Asian titles, especially those from China and Korea.

OSAC also supports ad hoc special requests from commands. For example, it arranged the purchase and delivery of several Mexico City telephone directories to the U.S. Northern Command (NORTHCOM) through the embassy procurement officer. OSAC initiated the process after contact by NORTHCOM and after verifying availability, cost, and shipping methods before handing completion of the transaction directly to the embassy and NORTHCOM.

Boundless Opportunities

With its mandate to build a community enterprise through a distributed architecture of OS collection and exploitation across the government, the OSC hopes to work with the COCOMs and the entire DOD to deconflict strategies and minimize redundancy. In conjunction with colleagues across the OS community, the Center will develop and provide a number of centralized services that will include tradecraft training, the building of common procedures and policies related to such issues as copyright and use of the Internet, and content procurement. The OSC is exploring the viability of detailing an OS officer to a command to learn more about how the commands operate and to test the viability of on-site support that has direct reach back to the Center. Meanwhile, ASD and OSC are considering the possibility of a personnel exchange on the small-unit level to achieve similar goals. Such forward deployment and personnel exchanges are the natural next step toward a broader and deeper partnership between OSC and the DOD. We look forward to the not-so-distant future when DOD uniformed and civilian personnel are working side-by-side with colleagues from across the community in the OSC.

The Open Source Academy Helps the Intelligence Community Make the Most of Open Sources

Editor's Note: There are four articles from the DNI Open Source Center in this issue of MIPB. Two of the articles, DOD and the DNI Open Source Center–Building the Partnership and The Open Source Academy Helps the Intelligence Community Make the Most of Open Sources, are unclassified. The other two articles, History of Open Source Exploitation in the Intelligence Community and OpenSource.gov, are FOUO and can be found on the sensitive but unclassified (SBU) "side" of MIPB. Request a user's account to read these and other articles at the MIPB Home Page, http://www.umi-online.us/mipb. For more information on the Open Source Center, call Customer Service at 1.800.205.8615.

by Douglas Peak

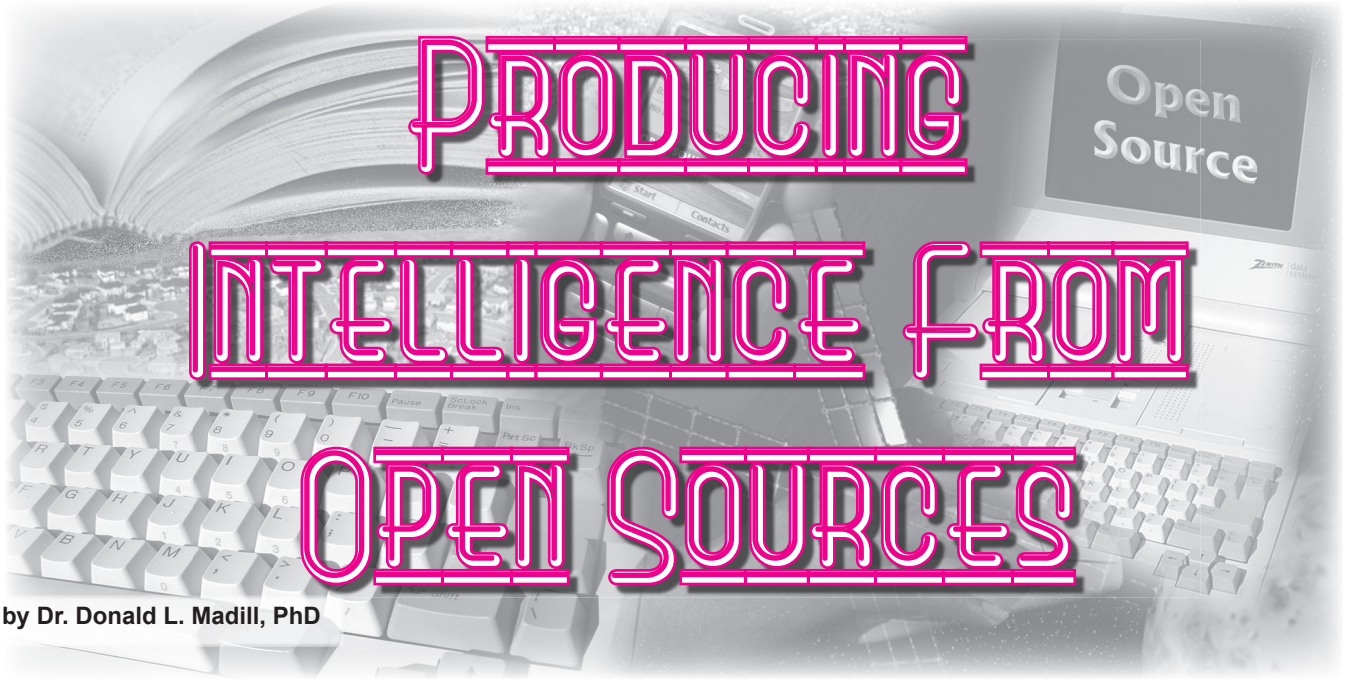
The Open Source Center's (OSC) Open Source Academy (OSA) has won recognition as a leading provider of OS tradecraft training in the Intelligence Community (IC) since its establishment in 2003. Intelligence consumers are placing a greater value on open source intelligence (OSINT), prompting OS specialists from the IC, policy and military communities, and other federal government organizations to take advantage of OSA courses to build their OS skills.

The Academy's core curriculum includes instructor-led courses on a growing range of topics including basic tradecraft, Internet exploitation, and reviewing finished intelligence products. OSA Provost Dave Kraus explains that there is more than meets the eye to using OS data. He says, "Our analytic tradecraft courses teach how to analyze the media, including ownership of media organizations and their political leanings. The courses on Internet exploitation go beyond the casual search skills that we've developed at home and in school. There are very precise search and research strategies, that are not intuitive, to cull valuable information from the Internet."

In response to the need to develop OS expertise throughout the IC, the OSA welcomes participants from all government organizations including the armed forces and law enforcement. As of November 2005, the Academy has hosted 88 participants from the Air Force, Army, Marine Corps, Navy, DOD's Counterintelligence Field Activity, Department of Homeland Security (DHS), Defense Intelligence Agency (DIA), Department of Treasury, Department of State, National Geospatial Intelligence Agency (NGA), National Reconnaissance Office (NRO), and National Security Agency (NSA). Even BBC Monitoring, an OSC partner in the UK, has sent personnel to the Academy's courses. Mr. Kraus expects attendance to grow as the OSA increases its outreach efforts and introduces new courses.

The courses that have attracted the highest interest include: ***Hidden Universes of Information on the Internet, Security and Privacy for Internet Users, Introductory Analytic Tradecraft***, and the seminar series co-sponsored with George Mason University on ***Understanding and Analyzing Global Media***. Multiple guest students have also attended ***Assessing Media Environments, Classification Workshop, Dissemination Platforms, Introduction to the Field, Media Analysis, Orientation to the Open Source Center, OSINT and the Other INTs***, and ***Overview of the OSC Collection Requirements Process***.

To obtain a copy of the OSA Course Catalog, register, or request information on OSA's other services, please contact the OSA Registrar at 703.613.5090.



Producing Intelligence from Open Sources

by Dr. Donald L. Madill, PhD

Introduction

During Senate hearings in 1947, experts from the Intelligence Community (IC) testified that a proper analysis of information gained through open sources could satisfy at least 80 percent of our peacetime intelligence requirements. [1] Since then, the Cold War has come and gone; formerly closed societies have begun to allow us access to information that was previously state secrets. The "Information Superhighway," with all its international connections, has given us access to much more information; there are few roadblocks or restricted-access routes for those who know what to look for and where to look for it. Under these conditions, the percentage of requirements that can be satisfied from open sources should be at least as great in the twenty-first century as it was in 1947.

Yet, open source intelligence (OSINT) has remained a discipline that the IC has often overlooked and underestimated. There has been little thought of a concerted effort to produce and disseminate unclassified intelligence products based on a systematic analysis of the masses of unclassified information available. Most intelligence organizations still regard open source data merely as background information. It rarely proceeds beyond the collection and processing steps of the intelligence process. In recent years, the Department of Defense (DOD) has defined *OSINT* as "Information of potential intelligence value that is available to the general public." [2] However, this definition would better fit the term *open source information*, since unprocessed, unevaluated information is not yet intelligence. No amount of information beautifully collected, indexed, and filed is of any value until analysts select what is pertinent, find out its meaning, put it together in a finished intelligence product, and communicate it to those who need it.

Today, there is a great need for unclassified intelligence products to satisfy known or anticipated intelligence requirements. To many, however, "unclassified intelligence" would seem to be an oxymoron, since we tend to associate "intelligence" with clandestine means and covert operations to obtain information about a foreign entity that did not intend for us to have this information. However, no official definition of *intelligence* says that it has to be classified. We often forget that not just high level decisionmakers and planners, who can use intelligence at various levels of classification, have legitimate requirements for information about our potential adversaries, emerging technologies, and other conditions in our operational environment (OE). Therefore, much of the information about the OE remains buried inside classified documents or unexploited in neglected open sources. Unfortunately, that prevents it from being readily available or useful to a large segment of potential consumers who must rely on unclassified information when operating in non-secure environments.

The irony is that our analysts and producers of foreign intelligence *could* obtain much of the same foreign intelligence information from open,

unclassified sources if they would merely look for it there. All the more ironic are cases where they *do* have access to the open source information but simply do not have a current mission to convert it into unclassified intelligence. By failing to take advantage of the wealth of material available in open sources, we expose the U.S. Army to the consequences of training and preparation based on inadequate knowledge of potential enemy capabilities or other characteristics of the OE in which we might find ourselves. This article discusses past efforts and lessons learned about how to apply all the steps of the intelligence process to the production of intelligence from open sources.

Historical Perspective

As early as the 1970s, the Defense Intelligence Agency (DIA) recognized the value of open sources. It had a special Handbook and Tactical Analysis Section dedicated to the production of unclassified intelligence. By 1979, the DIA had produced a variety of unclassified handbooks on the Soviet Ground Forces, primarily to support U.S. Army Training and Doctrine Command (TRADOC) requirements. At that point, TRADOC tasked DIA to produce a definitive unclassified intelligence document on the Soviet Army. This multivolume document was to serve as a comprehensive baseline reference to support threat instruction and training at TRADOC schools and centers, as well as the Opposing Force (OPFOR) Program throughout the Army. To ensure widest dissemination, the required document would not appear as a DIA publication, but rather as a field manual (FM) under the Armywide Training and Doctrinal Literature Program. Since DIA does not produce FMs, it agreed to provide TRADOC a draft document that updated and combined previous DIA unclassified handbooks into a single authoritative reference on Soviet operations, tactics, organizations, and equipment.

Within TRADOC, the Threats Directorate of the U.S. Army Combined Arms Center (CAC) at Fort Leavenworth received the DIA draft in 1981 and began to mold it into a final FM format. Intelligence analysts at CAC Threats, accustomed since 1976 to analyzing open source information on the Soviet Army, coordinated several substantive improvements with their DIA counterparts. This collaborative production effort culminated in 1982, with the published coordinating draft of FM 100-2 in three volumes. [3] Unfortunately, DIA had to discontinue its unclassified production effort in 1982, due to other priorities.

CAC Threats carried the FM 100-2 series through to final publication in 1984, making some further improvements based on emerging open source information. Many customers, as well as analysts in the Army's intelligence production centers, were surprised by the manuals' thoroughness and accuracy. In many cases, they learned that essentially the same information they were accustomed to seeing only at the sensitive compartmented information (SCI) or collateral classified levels was also available from open sources. Moreover, these unclassified products could enjoy wide dissemination throughout the Army and other services.

In 1985, CAC Threats began negotiations with intelligence production agencies to elicit their support for updating the FM 100-2 series. Previous DIA counterparts recommended that CAC Threats seek support from the then newly formed Army Intelligence Agency (AIA), which at that time controlled all the Army's intelligence production centers. However, AIA too had other priorities and had neither the staff nor the plans to provide input up front as DIA had done. Because of the great success of the original 1984 version, AIA directed that CAC Threats continue to produce and update the FM 100-2 series based on unclassified sources. The key role of CAC Threats in the intelligence and threat support (I&TS) community and its interface with users in the Army training community gave it a unique ability to tailor its unclassified products to user requirements.

By 1991, CAC Threats had updated two of the three volumes on the Soviet Army. Just at that time, however, the Soviet Union and its army began to break up, and the CAC and TRADOC commanders decided to discontinue the FM 100-2 series. To replace it, they directed CAC Threats to produce a new FM 100-60 series on a capabilities-based OPFOR for use in all Army training venues. [4] CAC Threats analysts continued to use previously established methodology to build a composite of foreign capabilities through the collection, processing, and analysis of open source information to produce and disseminate an unclassified intelligence product.

A reorganization in 1994 made the former CAC Threats directly subordinate to the TRADOC Deputy Chief of Staff for Intelligence (DCSINT), who was now the responsible official for the Army's OPFOR Program. This merger solidified the role of the TRADOC DCSINT organization in producing unclassified intelli-

gence to support training. In 2000, TRADOC DCSINT began to replace the FM 100-60 series with the new FM 7-100 series describing an OPFOR that helps represent the challenges of the contemporary operational environment (COE). [5] TRADOC DCSINT has also supported mission rehearsal exercises for units preparing for deployment in Afghanistan and Iraq by producing unclassified assessments of those particular operational environments.

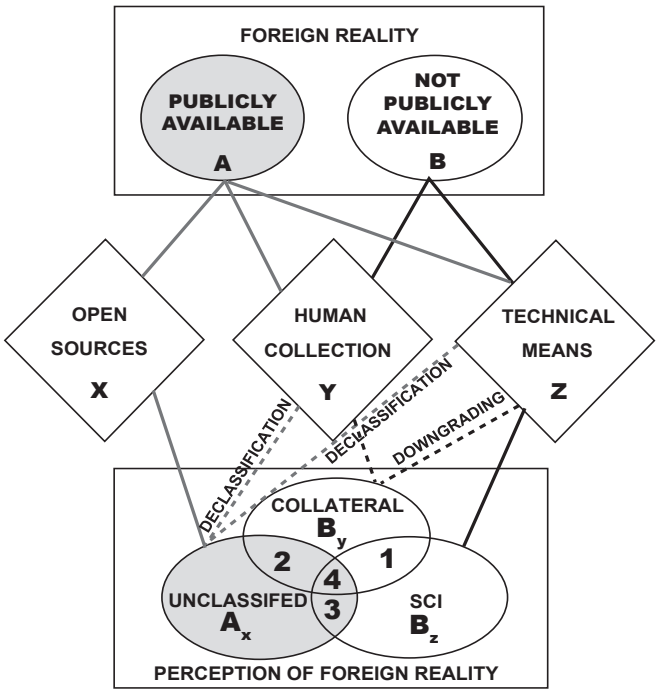
Steps in the Open Source Intelligence Process

Collection

The basis for all foreign intelligence is the *reality* that exists in the foreign environment. We may become aware of this foreign reality by a variety of means. These include open source collection: acquiring material in the public domain, such as unclassified foreign government documents, books, magazines, newspapers, and scholarly and trade journals, as well as monitoring foreign radio and television broadcasts and the Internet. Another collection source is human intelligence (HUMINT), where the information comes from human sources and is usually collected by sensitive means. Finally, there are technical collection means such as imagery intelligence (IMINT), measurement and signature intelligence (MASINT), or signals intelligence (SIGINT). Figure 1 shows the relationships between foreign reality, the U.S. collection means through which we are able to perceive that reality, and how this affects the classification of U.S. perceptions in products derived from the collected data.

Intelligence collectors normally classify raw foreign intelligence information according to the sensitivity of the sources and means through which they collected it. That source may be information that is not publicly available (marked B in Figure 1) and accessible only through highly sensitive, technical means (Z), in which case they would classify the initial report as SCI (B_z). If the source is still not publicly available (B), but collected through less sensitive covert means (Y), they would classify the initial report at the collateral level (B_y). If the source is publicly available (A) and acquired by overt, open source means (X), the initial report can be unclassified (A_x).

Besides that, analysts in the originating intelligence agency can downgrade the classification of information that subsequently becomes available from less



Areas of Overlapping Coverage

$1 = B_y + B_z$

$2 = A_x + A_y$

$3 = A_x + A_z$

$4 = A_x + A_y + A_z$

Figure 1. Collection Means and Perceptions of Foreign Reality.

sensitive sources. (This is exemplified by the overlap of B_y and B_z in Figure 1.) Likewise, the analysts of the originating agency—if they want—can declassify a piece of information previously published as classified, once it becomes known from open, unclassified sources (A_x), since its revelation would no longer compromise any sensitive source. Of course, it would be necessary to sanitize the downgraded or declassified version, eliminating references to the original, more sensitive source.

Open source information, whether it stems directly from foreign open sources or comes indirectly through government or nongovernmental collectors of open source data, can obviously be unclassified. (A possible exception might be open source information collected during a covert operation.) However, sensitive U.S. collection assets can collect foreign information that is publicly available (A_y or A_z) as well as foreign information that is not (B_y or B_z). Collectors using these

classified means often are incapable of ascertaining whether the information they perceive can also be perceived in another, unclassified mode (A_x). Because of this overlapping coverage, it is quite possible for raw intelligence information to be overclassified. For example, a HUMINT agent or defector might report information he read in a foreign newspaper. If an intelligence agency had a subscription to the same newspaper and screened it for such items, it could acquire the same information without involving a sensitive source. By SIGINT technical means, we might intercept a message from a foreign official attending an international conference, and the same day the same official might hold a news conference or issue a press release to the public media containing the same information. When we do collect the same elements of foreign information overtly through open sources, we can and should identify them as unclassified.

In determining collection requirements and priorities, information from open sources can influence both classified and unclassified efforts. Sometimes, publicly available information may contain all but a small percentage of the information consumers require. In that case, an intelligence organization with the nearly complete unclassified picture could task collectors to look for the missing pieces. That small, but important percentage that a foreign entity kept secret, if acquired by sensitive means, could be the basis for a key classified product. Once aware of the missing content, which the foreign entity might not regard as secret, collectors and screeners of open sources could be on the lookout for the same information in unclassified form. On the other hand, organizations dealing primarily with classified information might inadvertently run across pieces of unclassified information that could fill in gaps in the existing unclassified picture. Those responsible for guidance and direction of the overall intelligence process must ensure that there is a mechanism for systematically sharing such unclassified information with those who produce unclassified intelligence.

Processing

The processing step converts collected information into a form suitable for analyzing and producing intelligence. For open source information from foreign sources, this often involves the transcription and/or translation of foreign language material. Data from open sources also must go through a process of screening, sifting, and sorting. This initial analysis can occur in the processing step, when screening analysts review raw information in order to identify significant facts for subsequent interpretation. Not all raw information collected is pertinent, credible, or accurate. Because of the vast amounts of information available from open sources, it is inevitable that much of this great mass of data is not really useful for intelligence production or duplicates information already held. So, the problem is to sift out those potentially useful bits of unclassified information that are both new and significant. Only then can information collected from open sources become truly useful to analysts involved in intelligence production.

Even back in 1947, those intelligence experts testifying before the U.S. Senate pointed to “the increasingly vast quantities of foreign intelligence information that are becoming available” through open sources. They clearly recognized the potential value of this previously untapped source or raw information. However, they also realized that the “virtually staggering” volume of the material obtainable by these “overt, normal, and aboveboard means” was a potential barrier to exploiting it. Furthermore, they understood that a “proper analysis” of this material could be much harder work than its classified counterpart. Hence their frequent references to the need for “a thorough sifting and analysis of the masses of readily available material” and “the painstaking study of that available overt material.” [6] Since 1947, the volume of open source information has, of course, greatly expanded. This has further complicated the task of screening and analyzing.

Screening analysts or other trained intelligence workers must also determine whether a particular piece of information is pertinent to known or anticipated production requirements. Then they must ensure that any analyst producing intelligence to meet a given requirement has access to all the potentially valuable information pertaining to that requirement. The best intelligence data, classified or unclassified, are worthless if the intelligence producer is unaware of them.

Production

The production step converts information into intelligence through the evaluation, integration, analysis, and interpretation of all available data, including that from open sources. It also entails the preparation of finished intelligence products in support of known or

anticipated user requirements and in a form the user can apply. The finished product may be classified, unclassified, or a combination of the two—depending on user requirements.

One prerequisite for production is the **evaluation** of raw information for reliability of the source and accuracy of the content. The reliability of open sources can vary greatly—from government documents, to professional and technical journals, to news magazines, to hastily prepared newspaper reports. That is not to say that government documents are always accurate or that newspaper reports are always suspect. As with any intelligence source, analysts who deal most directly with these sources on a regular basis are the best judges of reliability. Thus, it might be a collector or a screening analyst rather than a production analyst who gauges reliability. However, the production analyst's personal knowledge of the subject matter and comparison with information on the same subject from other available sources are normally necessary to establish the accuracy of the information itself.

Many producers and consumers of intelligence often assume that the most reliable information is that which has the highest classification. That is not necessarily the case. In some instances, the unclassified information from open sources turns out to be the most reliable. The ultimate sources of unclassified intelligence may be what foreign entities say or show graphically about themselves in the open press, news broadcasts, sales brochures, or the Internet. These can rank among the most reliable of sources, when properly evaluated and analyzed. Open source data can often be just as accurate as information from classified sources. In some cases, the unclassified may be even more accurate, when the basis for the classified version was a guess, a mistaken interpretation, or outdated information.

There may be cases where a foreign entity purposely attempts to mislead us by providing false information. What usually leads to incorrect information, however, is our own misinterpretation of whatever data the foreign entity allows us to obtain through open source channels. This is why we need trained intelligence professionals involved in the production of data from open sources to support unclassified intelligence requirements. Non-intelligence customers, if provided only the unevaluated raw data, are likely to misinterpret it or be misled by faulty information.

Intelligence production also involves an **integration** function in which the analyst attempts to form a pattern by selecting, synthesizing, and combining evaluated information and previously developed intelligence. As the pattern emerges, the analyst often determines that some of the pieces are missing. Having identified these gaps, the analyst can then attempt to acquire additional information to complete, confirm, or refute the emerging pattern. If the desired intelligence product can be classified, data from sensitive sources may fill these gaps. If the product must remain unclassified, the analyst must find the missing pieces in open sources, get someone to declassify them, or provide a product that is useful though incomplete. There is always the possibility of refining the product at a later time, when more information does become available at the unclassified level.

Some would say that a compilation of material from unclassified sources runs the danger of becoming classified. This can indeed be true in the case of information about own systems and capabilities. The advantage of compilations of data is that they present a more complete picture of the situation than do the individual, isolated pieces of information of which they are constructed. Thus, a compilation of facts about us might draw a picture all too closely resembling the U.S. reality that we need to protect based on the possible damage to our national security that could result if our potential enemies knew these things about us. Generally, however, this does not seem to apply to foreign intelligence.

In the foreign intelligence business, we classify things primarily to protect our collection means. When information about a foreign entity becomes available from sources other than our own sensitive collection means, there is usually no need to classify it. If individual facts about the foreign entity are unclassified, then so are compilations of those facts. When intelligence analysts fit together bits and pieces of open source information analytically to form a greater body of unclassified information, the product should be thought of as approaching foreign reality, rather than approaching a classified perception of the same reality.

Analysis and **interpretation** are close companions that may have begun before the actual production step. During production, however, further analysis determines the significance of the information relative to

information and intelligence already known. Interpretation involves drawing deductions about the probable meaning of the evaluated and integrated information. The analysis of unclassified information usually involves separating the few pertinent grains of wheat from a mountain of irrelevant chaff. This requires a combination of hard work and discriminating judgment. This judgment must come from qualified intelligence specialists who ideally should have a thorough knowledge of information available from all sources.

In reality, however, the classification of finished intelligence products often depends on the authors' awareness of sources. For example, when CAC Threats published the coordinating draft of the FM 100-2 series in 1982, two higher-level intelligence organizations expressed concern about possible security violations. One organization, which dealt primarily with intelligence from collateral sources, provided a list of 16 items it believed should be SECRET or CONFIDENTIAL. The other, which dealt primarily with SCI material, believed that one particular item should be classified at that level. The chief of the first organization promptly informed the latter that the item in question did not need to be at the SCI level, since it was one of the 16 items his organization held at the collateral level. CAC Threats analysts then produced multiple open sources for each of the 16 items in question, satisfying all concerned that the information could indeed be unclassified. This phenomenon led CAC Threats authors to create the diagram that appears in Figure 1—to explain conceptually how the same piece of information could simultaneously be held at classified and unclassified levels.

Authors who are aware only of SCI sources would naturally classify their product as SCI, unless there is a way to sanitize the information so as not to reveal the source. Likewise, authors who are aware of collateral sources would tend to classify their product as collateral. Even if these authors were aware that the same information was available through SCI sources, the mere presence of those sources would not determine the classification. The only reason for keeping the information at the SCI level would be to provide additional detail or to offer additional proof of its validity by identifying the additional, perhaps more trusted source. The same is true when a piece of information becomes available at the unclassified level. An author might still choose to report it as collateral or SCI in order to identify confirming sources that add to its credibility. Without the need for that backup information, however, the unclassified information could stand alone or as an unclassified portion of a classified product.

Unfortunately, those who deal primarily with information collected from classified sources are not always aware of whether the same information may be available from unclassified sources. If the analysts already have the information from normally reliable classified sources, they might not feel the need to look for it elsewhere. If such analysts happen to come across the same information in open sources, they do not necessarily have to declassify the information previously acquired from sensitive sources, although that is an option. They also have the option of including in the classified product some unclassified text or photographs. However, the unclassified information, if incorporated into a paragraph or table also containing classified material, will no longer be identified as unclassified. This happens because our system of portion marking requires each portion to bear the classification marking corresponding to the most sensitive material it contains.

Dissemination

As we have just seen, there is no purpose in collecting intelligence information unless we subsequently analyze it and work it into a final product. Likewise, there is no sense in developing a final product if we do not disseminate it to those who need it *in a form they can use*. Thus, the dissemination of unclassified intelligence is mandatory to those elements of the U.S. military that need it to support training and other activities that for various reasons must remain unclassified. This means that someone has to provide the U.S. Army the best available unclassified information in an unclassified finished intelligence product.

A Job for Intelligence Professionals

Not just anybody with access to raw open source information can or should produce and disseminate intelligence-related products based on that information. At any level in the intelligence business, only trained, experienced intelligence professionals *should* do this, because only they *can* do it properly. "Properly" means ensuring that the best available information reaches non-intelligence customers at a level of classification that is usable for them.

We do not want non-intelligence customers "doing their own thing" in unclassified intelligence produc-

tion and coming up with their own versions of foreign intelligence data because intelligence professionals are not doing it for them. Otherwise, we could have problems with classified data showing up in unclassified products and data bases or unverified data giving the threat or OPFOR unrealistic capabilities—either overstated or understated.

Ideally, the same agency that produces classified intelligence should also produce as much unclassified intelligence as possible on the same subjects. Both classified and unclassified products would be validated and authoritative to the same degree, although possibly for different purposes. However, most analysts in those agencies already have a full-time job keeping up with classified production requirements to meet the needs of other, higher-priority customers. Those analysts also are generally not in a position to systematically screen unclassified sources and may not know what is or is not already known about a particular subject at the unclassified level. A more practical solution, therefore, might be for a separate group of intelligence specialists to produce unclassified products in concert with the agency's classified work.

Another possible solution is for intelligence specialists in an I&TS organization (such as TRADOC DCSINT) to produce the unclassified products, since they are most familiar with the needs of the Army training community and other potential users of unclassified intelligence. They can concentrate on exploiting open sources to meet those needs. This takes a group of experienced analysts whose primary focus is on the unclassified and who know the ground rules for unclassified intelligence production. These intelligence specialists must establish and maintain an adequate base of unclassified knowledge of the foreign areas and entities involved. This includes the analysts' personal knowledge, as well as knowledge of other intelligence products on the same subjects and the ability to coordinate with higher-level intelligence production agencies.

Another option for getting good unclassified products based on open sources is in a collaborative effort between intelligence production centers and I&TS specialists (similar to the past relationship between DIA and CAC Threats). This could involve the production centers providing validated and authoritative unclassified information from which the I&TS organization creates the final product tailored to customer needs.

In any of the above options, analysts focused on the classified production effort could still have ready access to unclassified products. Ideally, they would have the opportunity to review and comment on the unclassified products before dissemination. Occasionally, they might find a use for the unclassified information within their own products. In turn, those focused on unclassified production would have access to any unclassified intelligence produced by their own or other agencies and could tailor it for use in their own unclassified products. Thus, the two elements for classified and unclassified production can profit from each other's work and close coordination between counterpart analysts.

Some would argue that intelligence personnel who have access to classified information should not produce unclassified products on the same subjects. However, this is like arguing that those with access to SCI should not produce collateral intelligence. In both cases, it is desirable for the producer of less sensitive information to be aware of all the information available, including that which has a higher classification than the analysts can use in a particular product, in order to make fully informed decisions.

Analysts might have two pieces of contradictory information from unclassified sources on the same subject. When selecting which unclassified piece to use within a product that is overall classified, analysts would obviously pick the one that fits best into the context of information from all sources. It represents the best available unclassified information. If the only available unclassified information seems to be incorrect or not close enough to information confirmed by reliable, more sensitive sources, it might be better not to report it, rather than misleading or misinforming the customer. The same informed decision should be made when creating an unclassified product to meet the needs of certain non-intelligence customers. Good analysts would not knowingly give the customer something that is not the optimal product. The product based on only the unclassified pieces of information might not match the classified picture in every detail, but it should be close enough not to be misleading.

Intelligence analysts who deal primarily, or at least regularly with information from open sources tend to have a much broader awareness of the whole spectrum of unclassified knowledge available. The answers to many of our questions about foreign military

capabilities and other parts of foreign environments are out there in unclassified form. We just have to know the right places to look and look there on a regular basis, so as not to miss them.

Conclusion

The foreign reality is the same, regardless of how we find out about it. This explains how some facts can be "classified" and unclassified at the same time. It merely means that someone went to a lot of trouble and expense to acquire from sensitive sources the same information that could be derived from open sources. Thus, open source information, properly analyzed, can be both a valuable and a cost-effective part of intelligence production. It is the job of intelligence professionals to exploit this goldmine of information, extract the useful nuggets with potential intelligence value, and refine them into finished intelligence products.

Endnotes

1. Committee on Armed Services, *National Defense Establishment (Unification of the Armed Forces)* Hearing, 80th Congress, 1st Session on S. 758, Part 3, April 30, May 2 – 9, 1947 (Washington, D. C: U.S. Government Printing Office, 1947), 492, 497, 525. The testimony cited here was by LTG Hoyt S. Vandenberg, then Director of Central Intelligence, accompanied by a written statement submitted by his civilian deputy Allen W. Dulles.

2. **Joint Pub 1-02, Department of Defense Dictionary of Military and Associated Terms**, 12 April 2001 (as Amended Through 31 August 2005), 388.

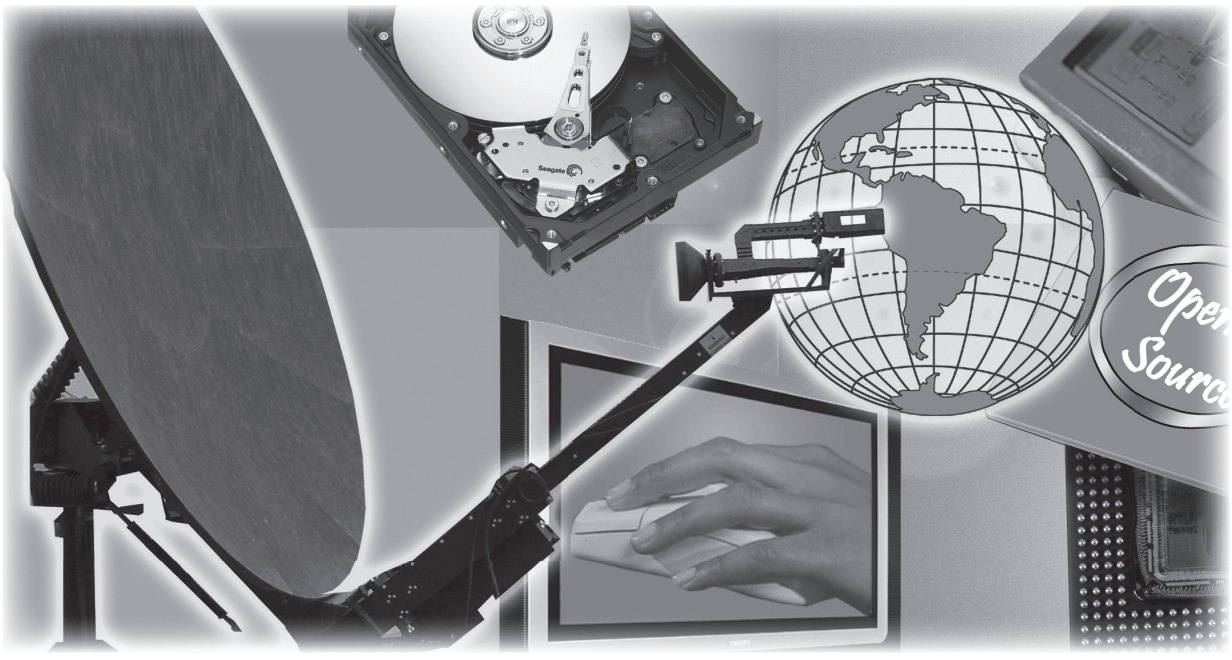
3. The **FM 100-2 Series** consisted of **FM 100-2-1, The Soviet Army: Operations and Tactics**, **FM 200-2-2, The Soviet Army: Specialized Warfare and Rear Area Support**, and **FM 200-2-3, The Soviet Army: Troops, Organization, and Equipment**.

4. **FM 100-60, Armor- and Mechanized-Based Opposing Force: Organization Guide**, 16 July 1997, **FM 100-61, Armor- and Mechanized-Based Opposing Force: Operational Art**, 26 January 1998, and **FM 100-63, Infantry-Based Opposing Force: Organization Guide**. 18 April 1996.

5. **FM 7-100, Opposing Forces Doctrinal Framework and Strategy**, 1 May 2003, and **FM 7-100.1, Opposing Force Operations**, 27 December 2004. Other FMs currently under development as parts of this OPFOR series include OPFOR tactics; paramilitary and nonmilitary organizations and tactics; organization guide; and worldwide equipment guide.

6. Committee on Armed Services, National Defense Establishment (Unification of the Armed Forces) Hearing.

Dr. Madill is currently a Senior Intelligence Specialist in the COE and Threat Integration Directorate (CTID), TRADOC DCSINT, located at Fort Leavenworth, Kansas. Prior to joining that organization (then known as CAC Threats) in 1978, he served as an enlisted SIGINT analyst in Vietnam and Germany and received a direct commission as an MI officer. At CAC Threats and CTID, he has co-authored the **FM 100-2 series** *on the Soviet Army, the* **FM 100-60 series** *on a capabilities-based OPFOR, and currently the* **FM 7-100 series** *on OPFOR for the COE. He received a BS in Education from the University of Kansas, an MA from Emporia State University, and a PhD from the University of Kansas. Readers can contact him at DSN 552-3862, commercial (913) 684-3862, or E-mail donald.madill@us.army.mil.*



50 Years of Excellence: ASD Forges Ahead as the Army's Premier OSINT Unit in the Pacific

by David A. Reese

"When people think of Army OSINT, they think of the Asian Studies Center."

With these words, representatives from the Asian Studies Detachment (ASD) were introduced to the attendees at the First Army Open Source Intelligence (OSINT) Practitioners Conference hosted by the National Ground Intelligence Center (NGIC) in April 2005. Later that morning during a break, and before my turn had arrived to present the ASD mission briefing, one of the participants approached me and asked, "So what makes you guys so unique?" I jokingly answered, "Well, we're the only ASD in the Army, so by definition, I guess that makes us unique." Later that afternoon, my briefing answered a lot of questions, and the attendees came away with a much better understanding of the size and scope of ASD's mission and its capabilities, as well as the short and long term challenges that it faces. Still, many colleagues never get a true feel for what ASD is all about until they actually pay us a visit, and then the response is almost always an overwhelming, "Wow, I had no idea!" This article, of course, cannot possibly paint a complete picture, either, but I hope that it will, at the very least, raise the community's consciousness about the existence of ASD and the contributions the unit has been making to the Department of Defense (DOD) for the past 50 years.

Located on Camp Zama about 25 miles west of Tokyo, ASD is an element of the U.S. Army Intelligence and Security Command's (INSCOM) 500th Military Intelligence Brigade, and is the Army's Open Source Intelligence exploitation center in the Pacific. ASD's mission is to collect, analyze, and report foreign OSINT information in response to theater and National level intelligence requirements. The unit exists primarily to support the tactical intelligence needs of U.S. Army Pacific (USARPAC), but its products serve all military services, joint commands, DOD intelligence agencies, and other non-DOD customers as well, including the Foreign Broadcast Information Service (FBIS), the Federal Bureau of Investigation (FBI), the State Department, and non-governmental strategic "think tanks." ASD strives to set the standard for providing timely and value-added reporting on Asia, derived from the fullest possible exploitation of foreign open source information.

ASD had its origins in 1947, when it stood up as the Research and Analysis Group, Town Plan Group and Cartographic Unit of the G2 Geographic Section under General MacArthur's General Headquarters in downtown Tokyo. Over the years the unit changed names numerous times and moved back and forth between the former Camp Drake and Camp Zama, but eventually made its permanent home at Camp Zama in 1974. The unit had been known as the U.S. ASD since October 1981.

Today, ASD employs personnel with a wide variety of technical skills and talents. Its staff is comprised of 12 Department of the Army (DA) civilians (DACs), 77 Japanese nationals, 2 contractors, and a varying number of Army Reservists and National Guardsmen. Many of our staff bring with them extensive experience from private sector and government organizations in various countries.

ASD's Japanese national employees, all funded and contracted to the U.S. government by the Japanese government, make up the heart and soul of the operation. As the unit's linguists, collectors, analysts, translators, librarians, and administrative support personnel, these foreign nationals accomplish ASD's collection, analysis, and reporting mission. Altogether they provide ASD with language expertise in Bengali, Burmese, Chinese, Indonesian, Japanese, Khmer, Korean, Hindi, Malaysian, Ne-

ASD analysts research a wide variety of hardcopy and Internet source materials as they prepare OSINT based reports for publication.

pali, Russian, Tagalog, Thai, Uygur, and Vietnamese, as well as a handful of European languages.

ASD subscribes to over 400 international publications in hardcopy and digital format. However, not all open source materials used by ASD are acquirable through subscription. ASD obtains other materials through memberships in international research and friendship organizations, and also by direct purchase from foreign bookstores and publishing houses.

Mission of ASD

Some mistakenly think that ASD is a translation unit. On the contrary, ASD analysts research materials, extract information relating to specific intelligence requirements, and write reports directly into their native language (Japanese) without actually translating the materials themselves. ASD's translation section then converts the reports into English, and the DAC reports officers check these translations and perform the final editing and formatting before the reports are published as Intelligence Information Reports (IIRs), the unit's primary product. With the exception of some defense attaché reporting, ASD is the only unit in the Army that synthesizes and cites a large number of open source references in an IIR format similar to research papers or essays.

In addition to the IIR, ASD also produces a daily Force Protection and Situational Awareness Report (FPSAR), an e-mail product composed of a compilation of news article excerpts from foreign media websites throughout the Pacific area of responsibility (AOR). Unlike the IIR, which is more strategic in nature, the FPSAR provides U.S. forces stationed or deployed throughout the PACOM AOR and other travelers with current force protection or security related open source information. The IIRs and FPSARs are available on ASD's OSIS, SIPRNET, and JWICS websites. In addition, the FPSAR is also posted on FBIS website, the FBI-Honolulu's Law Enforcement Online (LEO) website, the Foreign Military Studies Office's (FMSO) World Basic Information Library (WBIL), and the AKO Intelligence Knowledge Collaboration Center. ASD's website was honored in 2004 when the unit received the "Best of OSIS Award" at the annual Intelink Conference in Boston.

ASD prides itself on its responsiveness to short notice, adhoc requirements levied by U.S. PACOM, USARPAC, U.S. Forces Japan, or U.S. Army Japan which can be satisfied through open source exploitation. Recent examples over the last couple of years include reporting on elevated tensions between China and Taiwan during the Taiwan presidential elections in 2004; security threats to U.S.; allied forces conducting humanitarian relief operations in Indonesia following December 2004 tsunami devastation; and strategy and tactics employed during the August 2005 Sino-Russian combined counterterrorism Exercise PEACE MISSION 2005. As testimony to the high value of OSINT analysis and reporting, ASD IIRs since 2003 have received 28 "Major Significance" evaluations from the Defense Intelligence Agency, NGIC, and the Air Force's National Air and Space Intelligence Center (NASIC) on topics ranging from North Korean underground facilities to Chinese Peoples Liberation Army Air Force air and space science and technology developments.

Challenges

The explosion of the World Wide Web over the last decade has had a tremendous effect on ASD's OSINT exploitation modus operandi. Approximately half of ASD's cited sources currently consist of Internet-derived information, and the percentage is steadily growing. ASD must meet the near-future challenge of increasing its Internet coverage while simultaneously protecting its Internet research from OPSEC threats. To this end, ASD has already begun looking at increasing and standardizing its use of OSIS when conducting Internet searches, which will allow for increased security and anonymity. ASD plans to install OSIS on all of its computers in 2006.

Another challenge that ASD faces is the digitization of its immense hardcopy library. The library currently holds almost 250,000 foreign-language newspapers, periodicals, journals, and books which occupy an entire building wing. The facility operates like any other library—analysts must

find materials of interest, check them out, and take them back to their workstations. Mr. Matt Parrish, Chief of ASD's Technical Information Branch, which is in charge of collections and archiving, sums up the digitization goal as follows: "We want to provide Internet access to all of ASD's holdings, some of which are sole-source information, to community members worldwide. Of course, the cost savings that this information sharing will provide to the Intelligence Community will be an added benefit!"

In addition, ASD is exploring the feasibility of entering the realm of audio-visual media analysis with the possible implementation of tools such as the BBN Broadcast Monitoring System, which enables continuous real-time monitoring, transcription, and machine translation of foreign language television broadcasts.

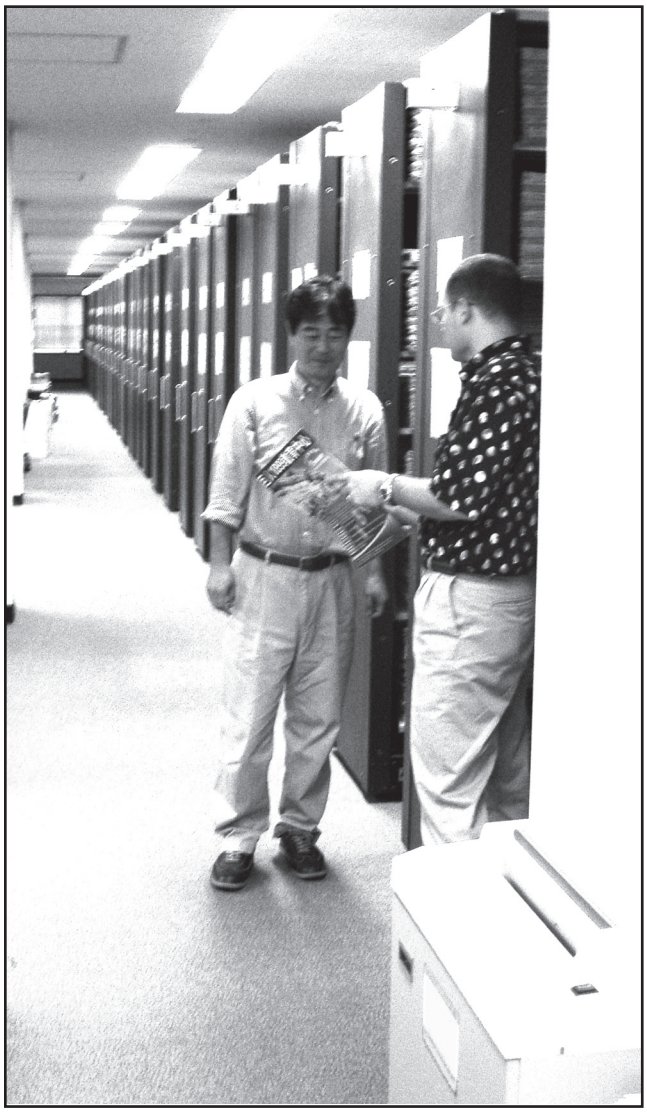
Partnership with FMSO

As part of the overall OSINT community's recent efforts at cooperation and collaboration, representatives from FMSO, DCSINT TRADOC, visited ASD in July 2005 to provide the Open Source Information Research & Analysis (OSIRA) Course to approximately 35 of ASD's DAC reports officers and Japanese analysts and translators. During the visit, ASD and FMSO discussed their commonality of missions and strategies. Says Mr. Don Wellman, ASD Director, "FMSO conducts research and produces products that are used at the highest levels of the DOD and U.S. government. FMSO's entrepreneurial approach to open source collection and reporting could be a great enhancement to ASD operations, and ASD and FMSO are exploring avenues for closer cooperation in the near future." Mr. Wellman visited FMSO in September 2005 to discuss the further development of a cooperative arrangement. He added, "Close cooperation between ASD and FMSO is expected to raise the capabilities of both organizations and improve the overall exploitation and utility of Army OSINT."

In addition, Captain Laura Levesque of the 10th Mountain Division G2 visited ASD in August 2005 to observe collection and reporting operations, particular by those related to the production of the daily FPSAR. Captain Levesque hopes to use what she learned at ASD in her own efforts to stand up an OSINT cell at Fort Drum, New York for deployment to Afghanistan in 2006.

All things considered, the large customer base, long history of conducting open source operations, multinational and multi-discipline workforce, resident language capabilities, wide product dissemination, and responsiveness to both strategic and tactical requirements, ASD truly is a unique entity in the OSINT community. The unit faces many technological and operational challenges, but is meeting and overcoming these challenges head-on. In doing so, ASD will continue to set the standard for excellence in the rapidly expanding and increasingly relevant field of OSINT well into the 21st century.

David Reese is the Operations Officer at the Asian Studies Center. He retired from the U.S. Air Force as an Intelligence Specialist in September 2000 and began working at ASD in October 2000. He holds an Associate of Applied Science Degree in Interpreting and Translating from the Community College of the Air Force and a BA in Business and Management from the University of Maryland. He is a member of the American Translators Association and the Japan Association of Translators. He can be reached at david.reese@us.army.mil or DSN (315) 263-5388.



Mr. Matt Parrish, Technical information Branch Chief, discusses ASD's library digitization initiative with Mr. Kiyoshi Tsukagoshi, Chief Librarian.

Open Source Information and the Military Intelligence Library

by Dr. Vee Herrington, PhD

"I work for the CIA. I am not a spy. I just read books!"

—from Three Days of the Condor

Most movie buffs remember this thriller made during the Cold War era involving a Central Intelligence Agency (CIA) researcher who reads books to find possible scenarios that could be used in intelligence work. This movie was about spies and espionage, but the spying involved no cloaks or daggers—the CIA agent just read books! The lead character was that of an ordinary, literary type, more like a librarian than a James Bond.

As the movie illustrates, intelligence does not have to be secret to be valuable. Open source intelligence (OSINT) incorporates all types of accessible and unclassified information sources such as books, newspapers, magazines, academic journals, government documents, radio, television, and the Internet.

Emerging Army doctrine states that relevant, accurate, and timely OSINT be provided to commanders at all levels. This is to be accomplished by integrating OSINT into all disciplines and functions by exploiting the Information Age to make OSINT a vital intelligence resource.[1] The research library is a vital link in this effort. This article shows how a new vision and model of library services transformed an under-used and under-funded library into a dynamic intelligence research center focusing on open source (OS) information and value-added services. The U.S. Army Military Intelligence (MI) Library [2] at Fort Huachuca, Arizona, illustrates the application of this model, meeting the information needs of the OSINT user and aligning the mission of the research library to the mission of the MI professional. This model moves the MI Library beyond the traditional role of a "place" to house books and other resources to a research center with value-added intelligence services.

All photographs courtesy of SSG MacCluskey and SPC Ereifej

The Research Library Mission

Historically, the mission of a research library has been to acquire information (the collection), organize it, preserve it, and make it available. The mission of the Intelligence professional is also to acquire and organize information; however, this information is then analyzed and turned into intelligence. Without getting into a formal doctrine definition, the simplest definition of intelligence can be attributed to Sun Tsu in *The Art of War:* "Know thine enemy." In order to win on the battlefield, intelligence about the enemy is necessary. For the MI Library to support the MI mission today, the library must focus on the Global War on Terrorism (GWOT).

Model Guidelines

Providing access to public or OS information has been the focus of libraries for hundreds, if not thousands, of years. Formats have evolved from the clay tablets found in ancient Mesopotamia five thousand years ago to the digital formats of today.[3] Unlike its classified counterparts (i.e., Human Intelligence, Signals Intelligence, Imagery Intelligence), OSINT draws from information found in the open, unclassified world of secondary sources. This is the world of the research library. Because of limited financial resources and the expense of information sources, the following guidelines were important considerations in implementing this new library model at the Army MI Library.

Create Enthusiasm

The model implemented at the MI Library called for a new library marketing and promotion strategy—a new vision of library services. Although one would think that this step should happen after developing the collection, it was important that the vision and marketing strategy happen early in the process. Many of the younger soldiers today do not appreciate libraries and actually want to avoid them. A wonderful OS collection can be built, but if no one uses the library or knows about the resources, then the effort has been in vain. If new soldiers beginning their career in Intelligence develop an enthusiasm and appreciation of the value of OS resources early on, they will utilize these resources even after leaving the schoolhouse.

This model calls for a new library "image" which better meets this generation's learning style. An article in College Student Journal describes this generation very well.

"The world of contemporary students is bombarded with noise, color, and action; even their entertainment is interactive and high tech. This new environment has impacted all levels of education." [4]

This statement is probably even more accurate when describing military students—they thrive on action or they would not have joined the military! The traditional library image is the opposite of what today's generation is accustomed to.

Utilizing this new vision of library services, the MI Library increased attendance by 850 percent by creating a new model of library service and pursuing a new marketing strategy. The vision for the MI Library is focused on a simple strategy: Get the customers to come to the library and create enthusiasm for using open source resources. Lure them in and then hook them! Change the image of the library. Make the library fun, comfortable, and relaxed. Create an environment that is extremely customer-focused.

"If you build it, they will come" does not always work. Some bookstore chains have transformed their image with great success—customers drink a cup of coffee and relax in a comfortable chair while reading books. Why would a profit based business allow customers to read the books without first buying them? Why would they risk having coffee spilled on the materials? The answer is simple: It is a marvelous marketing strategy which brings in the customers.

The marketing strategy of the MI Library includes briefings to all leaders, Open Houses, newsletters, class presentations, and library orientations.

Borrowing from the success of the chain bookstores, free coffee is always available to the customers. With comfortable chairs, music in the background, ice cream and soda machines, In-

ternet access, cable news, and videos, the MI Library attracts around 9000 customers a month. Before implementing the new library model, the MI Library was fortunate to have 50 customers a month. The soldiers may initially come for the coffee and ambience, but judging from the circulation increase of over 500 percent, they soon start reading journals, perusing the military reading lists, and checking out books. Eating is allowed in the library and many customers, utilizing the microwave, eat breakfast and lunch while studying. This library is a place where the customers never hear "Shh!"

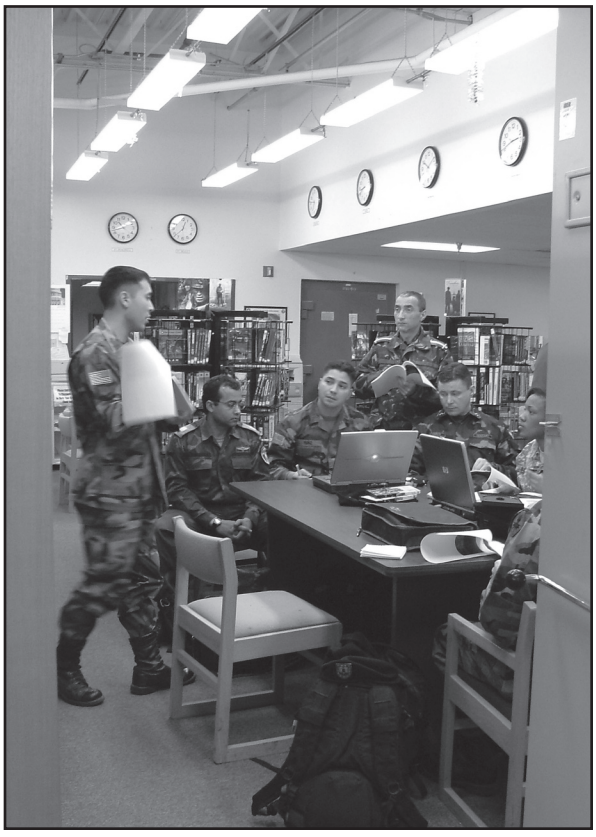
Tailor the Collection and Services

Tailor the collection to meet specific needs of the intelligence customer. Go for depth; not breadth. Consistent evaluation, feedback, and needs assessments from the OSINT user are necessary to meet the OS information needs created by such a rapidly changing world.[5] Research libraries, academic libraries, and special libraries are all similar because they do not attempt to collect everything; they do not try to be "all things to all people." The MI Library model proposes that the library focus on the present needs of the customers. What are the specific issues of the customer? What world events are taking place? How do these events impact the MI professional?

Continual needs assessments, surveys and evaluations of the existing services and resources are necessary to meet the needs of the customer. For example, before implementing this model, an evaluation of the present library collection at the MI Library found that 85 percent of the resources were over 25 years old with most focusing on the Cold War era. Based on an assessment of current world events and needs of the MI professional, an aggressive collection development plan was implemented in the areas of the Middle East and the GWOT. The customer surveys also indicated that longer hours were needed at the library since many of the MI customers could not use the library except at night. Library hours were increased by over 40 percent; the MI Library is now open 13 hours per day and on the weekend.

Provide Value-Added Services

Value-added services at the MI Library include an OS Lab with virtual private network (VPN) connectivity to the Open Source Information System (OSIS), instructional briefings in using OSIS, a National Geospatial-Intelligence Agency (NGA) Digital Map Library, and a Computer Center. To have an OS Lab is not enough—the value of OSIS as one-stop shopping for intelligence resources has to be aggressively promoted. Enthusiasm for OSIS is generated through class briefings, instruction, and OSIS demonstrations to include MI Corps leaders.



Almost 50 computers with Internet access are available to the customers, as excellent intelligence related sources are available via the Internet. Many of the students use the computers to write papers, build PowerPoint™ presentations, use FormFlow™

to fill out paperwork, take distance learning classes, book travel arrangements and take online surveys. A keyboarding tutorial program was even initiated at the library to assist the MI students who were having difficulty in class because typing skills slowed down their ability to write reports. Another popular value-added service is the new multi-media instruction room, with customers reserving this room for meetings, classes, role-playing activities, etc. Value-added services are not just the domain of the physical library, but can also be provided by the digital library through pathfinders [6], portals, and a virtual reference service. The heart of the "brick and mortar" library is its collections. However, the soul of the library is its vision, value-added services and customer focus.

Leverage Sources

Leveraging sources is another guideline in implementing the new library model. Simply put, this means that the MI Library does not purchase anything that can be obtained for free. Commercial databases are very expensive and most small libraries cannot afford the license or access fee. As depicted in Table 1, Army Knowledge Online (AKO) and OSIS licenses commercial databases. The MI Library leverages these sources and does not duplicate effort and expense.

Table 1. Commercial Fee-Based Databases.

Information Need	**Army Knowledge Online**[1] http://us.army.mil	**Open Source Information System**[2] http://www.osis.gov
Index for full-text journal, magazine and newspaper articles	*Academic Search Premier* *MasterFile Premier*	*Academic Search Premier*
Defense and Military Information	*Periscope* Military & Government Collection	*Jane's Online*
Country Studies	CountryWatch publications via Military and Government Collection	*Oxford Analytica* *ChinaVitae*
Terrorism	*Periscope*	*Jane's Online*
Global Analysis and Events		*Oxford Analytica* *Jane's Online*
World Economic and Business Indicators		*The Economist* *Oxford Analytica* *The Economist Intelligence Unit* (EIU Data Services) http://www.cosp.osis.gov/pages/eiu.htm

Note:
1. Accessing Databases via AKO. Login to AKO. At bottom left, click on Reference tab then Army Libraries tab to reach the Library Reference Center. Select title from "Databases and Resources by Title" (right frame).
2. OSIS Account and VPN Software. To access OSIS http://www.osis.gov a password and virtual private network (VPN) connectivity are needed. The OSIS link will not open until the customer has connected to the OSIS via VPN software. Passwords and VPN software can be obtained via AKO. Login to AKO. Do a search on "DA-IIS", which stands for the Department of Army Intelligence Information Services. This page guides the user to getting a password for OSIS and downloading the VPN connectivity software.

OS information also resides in many databases on the Internet. However, this information cannot be accessed using a search engine like Google. This information is considered "invisible" or "deep web" because it resides on a website designed around a database, there are no static pages to index (See Table 2 below). Some commercial vendors often create fee-based databases; with public information. For example, an 89 page thesis from the Naval Postgraduate School can be obtained for free by searching the Science and Technical Information Network (STINET) database. However, this same thesis is offered by several commercial vendors with a price tag of around $25.00.

Table 2. Deep Web or Invisible Web Databases.

Information Need	Location
Scholarly documents across disciplines	**Google Scholar**: Public Internet at http://scholar.google.com/ Google Scholar searches specifically for scholarly literature, including peer-reviewed papers, theses, books, preprints, abstracts and technical reports from all broad areas of research.
Lessons Learned: Intelligence	**Center for Army Lessons Learned (CALL)**: Public Internet at http://call.army.mil/ or use AKO password for FOUO. **Intelligence Center Online Network (ICON)**: Observations, Insights, and Lessons Learned (OIL): Public Internet with AKO password at http://iconportal.hua.army.mil
Scientific and Technical Information	**Defense Technical Information Center (DTIC)**: Public Internet with password at http://www.dtic.mil **DTIC Research & Engineering Portal**: Public Internet with password at https://rdte.osd.mil. **Scientific and Technical Information Network (STINET)**: Public Internet with password at https://dtic-stinet.dtic.mil/. This site is more restricted than DTIC.
Intelligence, Emerging Threats, Defense, and Military Information	**World Basic Information Library (WBIL)**: Research library located on OSIS and managed by the Foreign Military Studies Office (FMSO).
Worldwide Infrastructure	**Intelligent Road/Rail Information System (IRRIS)**: This is a web-based portal to worldwide infrastructure and real-time data. Public Internet with password at https://www.irris.tea.army.mil/irris/site/. Request account at https://www.irris.tea.army.mil/site/default.htm.
Intelligence: Field Manuals and Regulations	**Reimer Digital Library** http://atiam.train.army.mil/soldierPortal/appmanager/soldier/start?_nfpb=true&pageLabel=rdlservicespage
Intelligence: Doctrine and Training	**Army Doctrine and Training Publications**: Use AKO password. https://akocomm.us.army.mil/usapa/doctrine/34SeriesCollection_1.html
Note: Some database sites require registration or OSIS password.	

Exploit Technology

Although a cliché, this is the Information Age. Information, whether it is classified or open source, wins battle and wars. The library of the 21st century has no walls, no set hours, and no geographical constraints. Access issues are as important as ownership issues. The MI Library is both a physical "brick and mortar" library and a virtual library with information available anytime from anyplace. The physical library and the virtual library both develop collections. Traditionally, collection development has been defined as the planned purchase of materials in various formats to match the instructional and research needs of the customers. However, today these collections can be owned, licensed, or just accessed.

The virtual collection is just as important as the physical collection, but has different considerations and constraints. In addition to the library catalog pointing the customer to what is owned by the library, the Internet can be viewed as a gigantic catalog of information sources available worldwide. However, this information has to be tailored

to the information needs of the OSINT user. A value-added service to the customers is to sort and filter the myriad of online sources and create pathfinders and portals on the library website (See Table 3 below).

Table 3. Examples of Pathfinders and Portals.

Name	Location
Air War College	http://www.au.af.mil/au/awc/awcgate/awc-ntel.htm
Army War College Bibliographies	http://carlisle-www.army.mil/library/bibliographies.htm
Air University Bibliographies	http://www.au.af.mil/au/aul/bibs/bib97.htm

When possible, the collection should reflect both physical sources available in the library, as well as accessible digital sources. By exploiting technology, the library catalog of today not only reflects what is owned by the library, but also shows digital sources on the Internet. Even if a source is not owned by the library, it can be cataloged and accessed the same as an owned, physical source. With a click of the mouse, the online source or virtual reference is available.

The physical library collection is important if one lives or works near it. However, for most of us, a virtual library is necessary. The MI soldier transfers frequently to new locations and needs to consistently access sources regardless of geographic location. The MI Library provides a website with online access to the library catalog. A full time virtual model of library reference services is also available (Table 4 below). Collaboration and sharing of files via listserves and knowledge communities are important for the MI professional (Table 5 below).

Table 4. Virtual References.

Name	Location
Army Libraries Reference Center "Ask the Librarian"	Access through AKO "Reference"
US Army MI Library Virtual Reference "Ask A Librarian"	http://www.universityofmilitaryintelligence.us/mi_library/default.asp

Table 5. Communities and Listserves.

Name	Location
Intelligence Community	Access through AKO "Army Organizations"
Military Intelligence Information Sharing	intelst@pentagon-hqdadss.army.mil
Intelligence Center Online Network	Use AKO password http://iconportal.hua.army.mil
Community Collaboration Environment	Blogging and web publishing. Access via OSIS at http://www.osis.gov//cce/
Intelligence Community Library Consortium	Access via OSIS at http://web.iclc.osis.gov
Note: Some database sites require registration or OSIS password.	

In conclusion, Intelligence professionals are working in a different environment today. Stephen Mercado in an article in Studies in Intelligence says it best:

"Collecting intelligence these days is at times less a matter of stealing through dark alleys in a foreign land to meet some secret agent than one of surfing the Internet under the fluorescent lights of an office cubicle to find some open source. The world is changing with the advance of commerce and technology.

Mouse clicks and online dictionaries today often prove more useful than stylish cloaks and shiny daggers in gathering intelligence required to help analysts and officials understand the world." [7]

This article presents a model that moved the MI Library beyond the traditional role of a place to house books to a dynamic research center with value-added intelligence services and sources, such as an OS Lab. This model includes a new marketing strategy and image for the library which better meets this generation's learning style. By leveraging sources and exploiting technology, the MI Library is an important link in the MI Corps' effort to make OSINT a vital intelligence resource.

Endnotes

1 **INSCOM Open Source Intelligence (OSINT) Operations Handbook**, May 2003.

2 U.S. Army Military Intelligence Library URL: http://www.universityofmiltaryintelligence.us/mi_library/default.asp.

3 History of Libraries, at http://encarta.msn.com/encyclopedia_761564555_16/Library_(institution).html#s76.

4 Gary W. Howard, Holly Howard Ellis, and Karen Rasmussen, "*From the Arcade to the Classroom: Capitalizing on Students' Sensory Rich Media Preferences in Disciplined-based Learning*," College Student Journal 38, 3 (2004): 431-440.

5 Wyn Bowen, "*Open-Source Intelligence: A Valuable National Security Resource*," Janes Intelligence Review 11, 11 (1999), 50-54.

6 A pathfinder is a list of sources in a specific subject area.

7 Stephen C. Mercado, "*Sailing the Sea of OSINT in the Information Age*," Studies in Intelligence 48, 3 (2004). At http://www.odci.gov/csi/studies/vol48no3/article05.html.

Dr. Vee Herrington is the Chief of the U.S. Army Military Library at Fort Huachuca, Arizona. Past recent positions include Business Intelligence Specialist and Corporate Librarian for Lucent Technologies. In addition to a Master's Degree in Information and Library Science from the University of Tennessee, Dr. Herrington holds a PhD in Education from Arizona State University and a Master's Degree in School Psychology from the University of Cincinnati. Her other published works include "Way Beyond BI: A Look to the Future," Journal of Academic Librarianship, September, 1998 and "Toward a New Paradigm of Library Instruction in the Digital Library," 2nd European Conference on Research and Advanced Technology for Digital Libraries, September 1998. Readers can reach Dr. Herrington at vee.herrington@us.army.mil or the MI Library homepage at http://www.universityofmilitaryintelligence.us/mi_library/default.asp .

Editor's Note: The MI Library has been chosen by the Library of the Congress as the Federal Information Center of the Year for 2005.

Open Source Resources

This table contains some of the open source resources specifically tailored for the MI Library. These sources include the physical collection, as well as the virtual collection.

Type of Library	Focus of Library
Intelligence Research Library	Military Intelligence Terrorism National Defense

Information Need	Information Source	Location
Terrorism and Insurgency	*Jane's World Insurgency and Terrorism*. Hard and soft copy. *Periscope: Terrorism Database*	Purchase from Jane's. For the online version, access it via OSIS for free at http://www.osis.gov//Reference/janes/ Access via AKO Library Reference Center.
MI Training (Distance Learning)	*University of Military Intelligence (UMI)*	Public Internet, but password needed: http://www.universityofmilitaryintelligence.us/main.asp
Intelligence Exercise Products and Scenarios	*Intelligence Center Online Network (ICON)*	AKO Password needed: http://icon.army.mil
Cultural Awareness	*UMI Culture, Foreign Language, Integration Center (CFLIC)*	Public Internet at: http://www.universityofmilitaryintelligence.us/main.asp
Intelligence Products	*Marine Corps. Intelligence Activity*	Access via OSIS at: http://www.mcia.osis.gov/
Country Studies, Regional Security, and Defense Information	*FMSO*: The Army's Foreign Military Studies Office (FMSO) is a research and analysis center which conducts analytical programs focused on emerging and asymmetric threats, regional military and security developments, and other issues that define evolving operational environments around the world. *Jane's Sentinel Security Assessment.* *Jane's World Armies.*	Public version available at http://fmso.leavenworth.army.mil/index.htm Access FOUO site via OSIS: http://www.fmso.osis.gov/ Hard and soft copy. Purchase from Jane's or other book vendor. For the online version, access Jane's Online via OSIS for free at http://www.osis.gov//Reference/janes/
Scientific and Technical Sources and Research from Foreign Countries	*Spires High-Energy Physics (HEP)* Database Indexes over 500,000 articles, papers, preprints, and technical reports.. *E-Print Network* Search for foreign research in energy, science and technology.	Public Internet: http://www.slac.stanford.edu/spires/hep/ Index and access to high-energy physics technical papers from foreign countries. Public Internet: http://www.osti.gov/eprints/
Medical Intelligence	*Armed Forces Medical Intelligence Center*	Access via OSIS: http://www.afmic.osis.gov/

Information Need	Information Source	Location
Country Studies, Regional Security, and Defense Information	*Marine Corp. Country Handbooks* and other Products *Library of Congress Country Studies* *Library of Congress Portals to the World* *Library of Congress* USSR/Eastern Europe Foreign Press Survey (DBRIEF) *National Ground Intelligence Center (NGIC)*: Produces all-source integrated intelligence on foreign ground forces *DA-IIS* (Department of Army Intelligence Information System) Internet roadmap by country. National Defense University: MiPALs: U.S. policy statements.	For hard copies, contact INSCOM. For online access via OSIS http://www.mcia.osis.gov/ Public Internet: http://lcweb2.loc.gov/frd/cs/cshome.html Public Internet: http://www.loc.gov/rr/international/portals.html Access via OSIS: http://www.osis.gov/loc/eedbrief Access via OSIS: http://dadpm.inscom.osis.gov/ngic/list.htm Access via AKO: AKO → Army Organizations → Intelligence → DA-IIS Research Portal. Public Internet: http://merln.ndu.edu/index.cfm?type=page&pageID=3
Daily Intelligence Briefs and Reports	*Terrorism Literature Report*. *Terrorism Open Source. Intelligence Report.* *Swedish Morgen Report.* *Warning Intelligence on the Internet Review.* *Oxford Analytica* *Jane's Terrorism & Research Center*	Access via OSIS: http://www.osis.gov Access via OSIS: http://www.osis.gov/cgi-bin/rd?http://www.oxan.com/oxweb/ Access Jane's Online via OSIS: http://www.osis.gov//Reference/janes/
Research Studies: Military, Defense Focus, and Student Papers	*Air University Research Web*	Public Internet: https://research.maxwell.af.mil/index.aspx
Intelligence: Studies, Research, and Journal Articles	*CIA: Studies in Intelligence* *Military Intelligence Professional Bulletin (MIPB)*	Public Internet: http://www.cia.gov/csi/studies.html Public Internet: http://www.universityofmilitaryintelligence.us/mipb/default.asp
Imagery and Maps	*Google Earth*: World imagery and other geographic information. *National Geospatial Intelligence Agency (NGA)* *CIA Map Library* via OSIS *The Perry-Castañeda Library Map Collection*	Download free software from http://earth.google.com/ Access via OSIS: http://osis.nga.mil/ Access via OSIS: http://www-maps.osis.gov/ Public Internet: http://www.lib.utexas.edu/Libs/PCL/Map_collection/Map_collection.html
Strategy, Foreign Policy, and Defense	*Strategic Studies Institute* *Oxford Analytica* *Combat Studies Institute* *USAF Counterproliferation Center* *Digital National Security Archive*; Searchable database with access to once classified documents regarding U.S. Foreign Policy.	Public Internet: http://www.strategicstudiesinstitute.army.mil/ Access via OSIS: http://www.osis.gov/cgi-bin/rd?http://www.oxan.com/oxweb/ Public Internet: http://cgsc.leavenworth.army.mil/carl/resources/csi/csi.asp Public Internet: http://www.au.af.mil/au/awc/awcgate/awc-cps.htm Public Internet access at: http://www.gwu.edu/~nsarchiv/

Information Need	Information Source	Location
Gray Literature	*FBIS Gray Literature* *Combined Arms Research Library (CARL) Digital Library* Collections *GrayLit Network*:	Access via OSIS: http://www.cosp.osis.gov/graylit/ Public Internet: http://cgsc.leavenworth.army.mil/carl/contentdm/home.htm Public Internet: http://graylit.osti.gov/
Intelligence: Warfighter Systems, Electronic Warfare, and UAVs	*Jane's C4I.* *Jane's Radar & Electronic Warfare.* *Jane's Electronic Mission Aircraft.* *Jane's Unmanned Aerial Vehicles.* *Periscope* *Federated American Scientists (FAS)* *Global Security*	Purchase from Jane's. For the online version, access it via OSIS for free at http://www.osis.gov//Reference/janes/ Access via AKO: Reference → Army Libraries → Library Reference Center Public Internet: http://www.fas.gov Public Internet: http://www.globalsecurity.org/
Foreign Language: Foreign Media, Translation Tools, and Language Training	*FBIS*: Foreign Broadcast Information Service (FBIS). FBIS provides foreign media reporting and analysis. *University of Military Intelligence: Cultural, Foreign Language Integration Center (CFLIC)* *Defense Language Institute (DLI)* Foreign Language Center: Language Survival Kits *Google Translation* *OSIS Translation Tools* *Foreign Language Resource Center.* A database of Human Language Technology (HLT) software	Access via OSIS: http://www.osis.gov/cgi-bin/rd?https://www.OpenSource.gov/ Public Internet: http://www.universityofmilitaryintelligence.us Public Internet: http://oef.monterey.army.mil/downloadlsk.html Public Internet: http://www.google.com/language_tools Access via OSIS: http://www.osis.gov/about/machine_translation.html Access via OSIS: http://flrc.osis.gov/

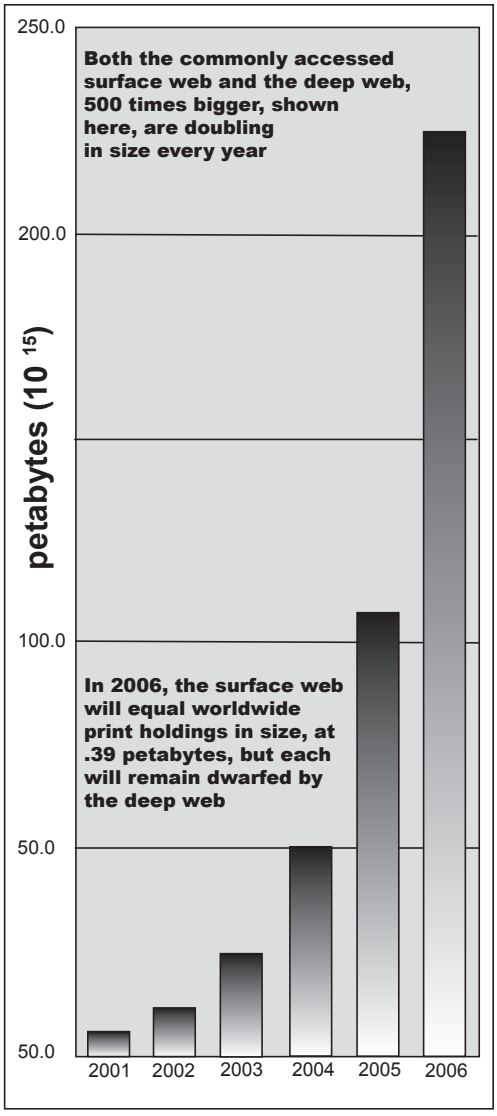
CREATING AN OPEN SOURCE CAPABILITY

by Lieutenant Colonel Joel J. Jeffson

John Gannon, former chairman of the National Intelligence Council, provided a fitting analogy describing what the Intelligence Community (IC) faces today when he told a story of the time he was standing watch on a Navy ship and heard one officer ask another as he scanned the horizon, "My God, have you ever seen so much water?" And the second officer replied, "Yes, and we only see the top of it!" [1]

Wading through this sea of information, caused by the proliferation of material available through the Internet, and reducing it to information analysts need without overloading them with data is a significant challenge to intelligence organizations. While the amount of classified information is increasing in a near-linear trend, the web is exponentially bringing open source (OS) information out of the hardcopy world of newspapers, periodicals, and specialized databases directly to the desktops of today's analysts.

As this rapidly increasing amount of public information became available to analysts, most organizations simply viewed OS as another tool in the analyst's kit bag, and left it to the individual to research and incorporate OS information as they saw fit. This naturally led to varying degrees of success, as some analysts readily took to incorporating this new information into their products while others were reluctant to use anything that did not come through their classified message handling system.



Introduction

The purpose of this article is to provide a roadmap for organizations considering establishing a formal OS capability to collect and process the information, beyond simply having individual analysts do their own research along with the rest of their duties. Developing this capability does not necessarily require creating a separate section, although that certainly helps; but it does require time and effort at the outset to make the program operational, and then less effort to monitor and maintain it.

The leadership at the U.S. European Command's (EUCOM) Joint Analysis Center (JAC) realized that the organization was not fully exploiting the vast amounts of publicly available information, and decided to create a section that would focus solely on finding OS information and pushing this information directly into the hands of the analysts. The section would also respond directly to the analyst's OS request for information (RFI), a capability that did not exist within the organization prior to the creation of the section and one that does not formally exist within the IC today.

An additional benefit of creating this section is that EUCOM routinely operates in a Coalition environment, and having a robust OS capability will greatly enhance the ability to share information with the various organizations, countries, and Coalitions that EUCOM works with. This is especially true for developing countries, which normally only operate with U.S. Forces on an ad hoc basis and with whom no formal intelligence sharing frameworks exist. OS material and unclassified information sharing systems are 'made to order' for information-sharing in a multinational-coalition environment.

Planning Considerations

Manning

How to man the section was the first decision that needed to be made, and the command decided to take a slightly different approach than others in the community. To ensure the section did more than just research the Internet and answer RFIs required experienced analysts who understood what their colleagues required and could proactively acquire this information and make it available to the analysts. This was not meant to be a slight to the research assistants and junior analysts who are often put in these positions, but it was felt that the more experienced analysts had a better understanding of the analytical requirements and would be able to focus their research on what was truly required and not what appeared interesting.

The decision was eventually made to select a senior analyst from each of three regional sections and one from the counterterrorism section. This way the OS section would mirror the rest of the analytical division, and each section would have a representative whom they knew well and had previously worked with to answer their questions. These analysts also work concurrently on longer term OS research projects in support of their home sections.

Requirements

Requirements drive all intelligence operations, and creating an OS capability should be no different. It was imperative to narrow down the requirements as much as possible early on, because one will quickly reach the point of information overload due to the vast amounts of information available. Once the program matures, the requirements can be expanded, but it is best to start with a narrow focus.

In addition to determining the requirements, it was important to identify what *not* to focus on. The decision was made up front that the section would not attempt to compete in the current intelligence environment. There are more than enough sources, classified and unclassified, currently available to analysts to satisfy their current intelligence requirements and updating the web sites would fully commit the section, with minimal time remaining to exploit new sources.

Current intelligence is important to commanders at all echelons, but more so at a tactical level and OS information might be one of the keys to satisfying this requirement. This is not to imply current intelligence is not an appropriate OS mission for all organizations, just that it is not a requirement for the JAC.

Dissemination

Identifying the method of dissemination that would reach the widest audience was the next step in the process. It is important to determine this prior to dedicating time actively searching for material. Posting products on a web site and making them available to all was quickly decided to be the most effective means of dissemination. Public folders and e-mail methods of dissemination were considered, but discounted. Public folders would only be of use to the organization and products delivered via e-mail would only benefit those on our distribution lists. Plus, both public folders and email have limited search capabilities, and do not

provide the analyst with an effective search capability, which is critical to effectively utilize the collected information.

The web site where the products are posted must reside on the network which the analysts primarily use when working on their products. At the JAC, for example, the decision was made to post products to the Secure Internet Protocol Router Network (SIPRNET) and the Joint Worldwide Intelligence Communications System (JWICS) networks, and not to the unclassified network. The JWICS is the primary system used by JAC analysts, and the SIPRNET is the main system used by the majority of EUCOM consumers. Furthermore, there are a limited number of unclassified workstations available at the JAC. If OS products cannot literally be put at the analysts' fingertips, they will likely not be used.

Mirror web sites also exist on Coalition networks. As mentioned earlier, a side benefit of OS information is that it can readily be shared with Coalition partners with minimal foreign disclosure concerns. The creation of a coalition OS site may encourage other nations to post their products to the site as well; potentially greatly increasing the amount of OS material available to U.S. organizations.

A portal on the unclassified network facilitates the analyst's individual research of the web. The site is similar to the Department of the Army Intelligence Information Services (DA IIS) site, in that it lists approved resources, links, and references tailored to the EUCOM area of responsibility. This site enables the analysts to effectively search the Internet, while spending a minimum amount of time trying to find information or determine if a site is credible.

OSINT on SIPRNET

Once a decision is made on requirements and means of dissemination, it is time to begin searching for relevant information. Surprisingly, the first place to begin the search for OS information is not on the Internet or the Director of National Intelligence's Open Source Information System (OSIS), but on the classified networks. The SIPRNET, and to a lesser extent the JWICS, contains numerous links to OS resources.

The Army OS Portal could be the best place to start your search on the SIPRNET. It has an *OS Products* section and an *Army OS Sites* section. These sections will lead you to numerous finished products, and to sites where individual units host their own products. Ideally, one of the commands' sites will match your OS requirements, and this will save a lot of time and effort by not having to duplicate the work that others have already done. Also, by reviewing the other units' sites, you can see how other organizations approach OS and gain insight on what may work best for your organization.

The DA IIS is another site on the SIPRNET that should be looked at. This site also provides links to numerous OS products and units hosting OS pages. Additionally, DA IIS also has a companion page with links to hundreds of indexed web sites available through OSIS.

A Running Start on the World Wide Web

Once the search of the Internet finally begins, a common mistake is to think that fee-for-service sites are required, but in the majority of circumstances this is not the case. It will quickly become apparent there are more than enough free or already-paid-for sites available, and the purchase of information by individual units is not required. Of course, there are exceptions for access to unique services or databases, and it is up to the individual unit to determine if it wants to spend resources on these services.

A good first site at which to begin your search for OS content is the OSIS homepage. OSIS is a virtual private network managed by the Intelink Management Office which provides authorized users access to unclassified and For Official Use Only (FOUO) information from both the U.S. Government and commercial sources. If your unit does not already have access to the OSIS network, contact them at info@center.osis.gov, and they can assist you in gaining access. For operational security (OPSEC) reasons, the site is not accessible directly from the Internet and requires password authentication for access.

The OSIS Homepage provides links to unique government sites that are accessible only through the OSIS network, such as the World Basic Information Library (WBIL), which contains basic and background information on 140 countries, the Marine Corps Intelligence Activity (MCIA) and the National Air and Space Intelligence Center (NASIC). The IC also provides authorized users free access through OSIS to premium content providers such as Jane's Electronic

Library, Oxford Analytica, EBSCO Host, Economist Intelligence Unit, and other services that would be cost prohibitive for organizations if they had to pay for the content individually. The site also allows you to customize live feeds from numerous worldwide news services directly to your desktop and, in addition to the links, contains handbooks and reference materials on how to best exploit OS material. Furthermore, in an effort to enhance the user's OPSEC posture, OSIS also provides *'protected access'* to the public Internet to allow OS research without divulging personal or organizational identities.

The Army Knowledge Online (AKO) Library Program site provides users another Internet tool with a wealth of information. By now, all Army soldiers are aware of AKO, but the fact that the library site exists, and what it contains, is not commonly known. Unlike OSIS, this site acts more as a gateway to informational type services that one would normally associate with that of a library, and is accessible directly from the Internet. AKO is not limited only to soldiers; non-Army government users and government contractors can also gain access to the site when sponsored by an Army user.

A separate article would be required to describe all of the products available at this site, but representative examples are *Country Watch*, which provides up-to-date political, economic, cultural, business and environmental information on 192 countries; and the *Student Resource Center* link, which provides access to the *Worldmark Encyclopedias* (providing world-wide coverage of geographic and cultural issues.) EBSCO Host is available on the AKO site, as well as on OSIS, providing access to thousands of journals which could contribute to more long-term intelligence issues.

One unique feature of the AKO library site is the *"Ask a Librarian"* link. If you experience difficulty trying to find a source or a specific piece of information, you can call on a professional research librarian for help. Simply type in your question, and you will normally receive a response within forty-eight hours. Regardless of where you are in the world at that moment, you will be able to receive assistance on whatever you are researching.

Other government library services are available beyond the AKO site. National agency libraries (Library of Congress, National Library of Medicine, etc.) and the libraries of military colleges and universities (Combined Arms Research Library, Naval War College, etc.) provide searchable sites and content. If the product you require is not available via the Web, many of them will loan the document directly to your command library.

Neither AKO nor OSIS are all-encompassing sites that will satisfy all requirements, but these sites need to be fully researched and exploited before any consideration is made to purchase content. While many premium content providers produce original content, the majority repackage much of the information that is already available from these two sites.

Beyond OSIS and AKO, the Internet provides a seemingly limitless amount of information that can support your mission. Once the search of the remainder of the Web begins, it is important to ensure that only quality sites are used. Reading *Untangling the Web*, available on the OSIS homepage, is recommended prior to searching in order to learn the best techniques to utilize the Web and to understand the potential pitfalls as well. There are numerous sites that look and feel like authoritative web sites, but are factually incorrect or biased towards a certain viewpoint that an unsuspecting analyst may not realize.

Beyond the World Wide Web

It could be a mistake to overlook the traditional brick-and-mortar library as a source for OS information. The quality and quantity of material will vary from location to location, but most libraries have access to inter-library loan programs, providing access to more resources than are available at your local branch as mentioned earlier.

Depending on your location and budget, private organizations and universities can provide another source for information, and these institutions are also rich in subject matter experts in their respective fields. The JAC has unique access to some world-renowned organizations, such as the Royal Institute of International Affairs and the London School of Economics, which frequently conduct seminars on topics of direct interest to EUCOM. Our analysts have the opportunity to attend these lectures and hear directly from world leaders and experts. If budget constraints or distance do not allow direct participation, many of these organizations provide e-memberships, at a much-reduced cost compared to full memberships, which may meet your needs.

Conclusion

There are certainly more open sources of information available to the IC today than there have ever been before, and the IC needs to be at the forefront in exploiting these sources to provide its consumers with greater clarity and depth of analysis. The challenge for anyone standing up a formal OS capability is to clearly define the mission requirements and then finding the sources to satisfy the requirements. A well-thought out plan from the outset is essential to assist in navigating the vast amounts of information available, and saving the one resource you can never have enough of—your limited time.

Endnotes

1. John C. Gannon, "*Strategic Use of Open Source Information*," *Vital Speeches of the Day* 67, Issue 5 (12 December 2000): 153.

Lieutenant Colonel Joel Jeffson is currently the Chief of the Open Source Section at the EUCOM JAC at RAF Molesworth, UK, where he was also the Chief of the Middle East/North Africa Section and Chief of the Strategic Estimates Section. He deployed in support of Operations IRAQI and ENDURING FREEDOM as the EUCOM J2 LNO to the CFLCC C2 and to Afghanistan as the CJSOTF J5 Intelligence Plans Officer. Previous assignments include ACE Chief and S3 in the 297th MI Battalion, 513th MI Brigade, Fort Gordon, Georgia; S2, 3/327th Infantry Battalion, S2, 1st Brigade, 101st Airborne Division (AASLT), and Commander, A Company 311th MI Battalion at Fort Campbell, Kentucky. Lieutenant Colonel Jeffson was commissioned through the U.S. Army ROTC and received a BS in History from the University of Wisconsin-La Crosse. He also has an MA in Strategic Intelligence from the Joint Military Intelligence College and an MA in Military Arts and Sciences from the U.S. Army Command and General Staff College.

The 2006 Army National Guard G2/S2 Workshop–Applauding Military Intelligence, A Total Team Effort

The Army National Guard will hold the 2006 Army National Guard G2/S2 Workshop on 7 and 8 April 2006, hosted by the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) at Fort Huachuca, Arizona. The focus of the workshop is "*Military Intelligence–A Total Team Effort*." This workshop will applaud the successes of Military Intelligence (MI) in the Army as the Army National Guard, U.S. Army Reserve and the U.S. Army Active Component teamed up to meet and fulfill mission requirements on the battlefield. The workshop will also explore ways to maintain these successes in the future.

Keynote addresses are scheduled to be provided by the Director of the Army National Guard, and the Deputy Chief of Staff, G2, Department of the Army. Insights will also be provided by the Commanding General, USAIC&FH, the Command Sergeant Major of the MI Corps, and the U.S. Army Forces Command G2. Briefings will be provided by a Division G2, a Brigade Combat Team S2, and a Tactical Exploitation Battalion commander from the Army National Guard, all of whom have recently redeployed from Iraq.

Teamwork is an essential ingredient for the success of any operation. A key component in this team effort is the support provided by all staff sections. Each staff section in an organization must not only understand the desired objectives but also how to achieve the end state. Cohesiveness among all staff sections is paramount to ensure mission success. This workshop will also focus on all the staff sections in the Army National Guard that enable MI mission success. Presentations are scheduled to be provided by Strength Maintenance, Training, Force Structure, Acquisition, and Operations organizations within the Army National Guard. Each of these organizations provides a valuable service to the readiness of MI in the Army National Guard.

Conference information and registration are available on the Guard Knowledge Online by accessing the Army National Guard link to the Operations Division, Intelligence and Security Branch web site, or by contacting Major Jaime Castillo at jaime.b.castillo@ng.army.mil

FMSO-JRIC and Open Source Intelligence: Speaking Prose in a World of Verse

by Dr. Jacob W. Kipp, PhD

The views expressed are those of the author and should not be construed to represent the views of the Department of the Army or the Department of Defense.

Introduction

There has been much debate about the role of open source information and Open Source Intelligence (OSINT) in national security since the events of 2001. The Intelligence Reform and Terrorism Prevention Act of 2004 calls for the newly created Director of National Intelligence (DNI) to create a "center for the collection, analysis, production and dissemination of open source intelligence to the Intelligence Community (IC)." [1] The Act further calls upon the DNI to ensure that the IC makes efficient and effective use of open source information and analysis and integrate open source intelligence into the national intelligence cycle.[2] In response to this interest and legislative action, the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) undertook a broad assessment of OSINT organization and practices within the Department of Defense (DOD) and reported that there was a lack of formal doctrine, policy, and design.

In response to this assessment, the OUSD(I) chartered the Defense Open Source Council (DOSC) to establish OSINT as an intelligence discipline. On the basis of his involvement with the OUSD(I) working group, Mr. Craig Manley, Department of the Army (DA) G2 Functional Coordinator for OSINT, noted the challenges before DOSC were significant and involved. The challenges included: developing a comprehensive understanding of open source requirements, developing an open source intelligence strategy for DOD, formulating an investment strategy, recommending a management construct, facilitating the development of open source policy and doctrine, and increasing DOD participation in IC-level open source forums.[3]

Given this increased interest in OSINT, the obvious first question is the definition of this type of intelligence. The classic definition of the intelligence process has been "the discovery of secrets by secret means." [4] The distinctive feature of the other forms of intelligence has always been the technical and human difficulties associated with the covert collection of materials and their application within the Intelligence Cycle (requirements definition, collection management, source discovery and validation, multi-source fusion, compelling presentation). OSINT differs from these in that it applies the Intelligence Cycle to the abundance of publicly available materials. Obtaining the materials does not pose a first-order problem. The primary task is transforming such source material into products that are useful for the IC and larger Joint, inter-agency, and inter-governmental communities.

The value of open source information has long been recognized by intelligence professionals. Robin Winks in his history of the relationship between academic research and intelligence made this point one of his critical conclusions. The two worlds share much in method but are distinct in product. They must share an equal commitment to civic virtue in a democratic society. The late Sherwood Kent, a leading practitioner and student of intelligence, spoke of the overwhelming majority of all information needed for the production of classified intelligence as coming from open source information, "of the things our state must know about other states some 90 percent may be discovered through open means." [5] In 1946, on the eve of birth of the modern U.S. IC, Kent noted the difficulty of defining intelligence, since the term was and is

The FMSO building at Fort Leavenworth, Kansas.

applied to both the craft and the product.[6] The product might better be called *knowledge*, and the Foreign Military Studies Office (FMSO) has been in that business since its founding. All-source intelligence, which includes the ten percent information, produces a special kind of knowledge that must be protected with varying degrees of classification and by what Churchill called a "body guard of lies." FMSO's products are a lesser but important sort of knowledge that can be used for the training and education of the force.

Cold War Origins of FMSO

The veterans of the FMSO, a small organization at Fort Leavenworth, Kansas, belonging to the US Army Training and Doctrine Command (TRADOC), have been producing unclassified intelligence since its founding during the Cold War.[7] They find themselves in a situation similar to that of Monsieur Jourdain, protagonist of Moliere's play, "Le Bourgeois Gentilhomme." Jourdain, anxious to ensure the successful pursuit of a lady of great rank and quality, seeks the assistance of the Philosophy Master to compose a note to that purpose. When told that he has two options, verse or prose, Jourdain is pleasantly surprised: "Well, what do you know about that! These forty years now, I've been speaking in prose without knowing it!" Instead of prose and verse, the Soviet Army Studies Office (SASO), the precursor of FMSO, confronted the choice of tasking it to provide unclassified or classified knowledge. As a result of that choice, FMSO has many years of experience in providing the former. In this case, the lady might be called funding, and the pleasant surprise was that unclassified knowledge was and is increasingly in demand.

Thus, FMSO's unclassified experience was the direct result of command intent. General William Richardson, then TRADOC Commander, created SASO on the model of the Soviet Studies Research Center at the Royal Military Academy Sandhurst, which was founded by Peter Vigor and then headed by Christopher Donnelly. It conducted open source analysis of the Soviet military for Britain's Battle Command Doctrine. General Richardson's intent was explicit—create an analogous research center to engage in the same process and in close cooperation with its British counterpart. He selected Fort Leavenworth as the location because of the critical role that the Combined Arms Center (CAC) played in the development of Army doctrine. FMSO's method was to conduct deep, mid- and long- term research on topics in order to create a context for understanding emerging trends in the Soviet military and state.

General Richardson sought to create a team of military and civilian experts to conduct such research, develop relevant archives of open source materials, and publish broadly to encourage debate and discussion of relevant aspects of Soviet doctrine, force structure, military art, history, and technology. The audience was to be the U.S. Army, the Joint Community, and the National Security Community. Taskings were to come from the Chief of Staff of the Army, the TRADOC Commander, and the CAC Commander. By common agreement, a fourth tasker was added: the Soviets themselves, with the

understanding that analysts would address new topics and subjects which emerged from the Office's deep study of Soviet open source materials. Publications were to be in the marketplace of ideas, subject to open debate and discussion. The military experts were to be drawn from Foreign Area Officers (FAOs) possessing knowledge of Russian, and having advanced civilian education and deep expertise on the Soviet military. Most were graduates of the U.S. Army Russian Institute in Garmisch, Germany. The civilian experts were to be drawn from academe with advanced graduate degrees in Russian studies and extensive publications on Russian and Soviet military history and affairs with many having broad experience in the Soviet Union and Eastern Europe. The concept depended upon a culture of mutual respect and support across the "two cultures" of academe and the professional military. The team concept was embedded in SASO's initial leadership, Dr. Bruce Menning served as director and Colonel David Glantz served as head of research. Both men encouraged close ties between SASO and the Army "school house," especially the Command and General Staff College (CGSC) and the School for Advanced Military Studies (SAMS). Their admonition echoed that of Moltke the Elder to officers of the Prussian General Staff to "be more than you seem." SASO served the Army well by providing a comprehensive understanding of Soviet operational art, tactics, and military doctrine.

The emblem of SASO, which is the basis of that of FMSO, had a Red Star and the single Russian word, "*znanie,*" (knowledge) upon it. The current emblem carries the globe inside a star with words for knowledge in ten languages surrounding the star. While the focus of FMSO research has become global, the method applied remains the same. The corpus of SASO's products is still available on FMSO's website or at the Combined Arms Research Library (CARL) at Fort Leavenworth.[8] Another key repository of SASO materials is *The Journal of Slavic Military Studies*, a quarterly scholarly publication, founded and still edited by David Glantz.[9]

FMSO and Post-Cold War World

With the end of the Cold War, the Velvet Revolutions in Eastern Europe, and the collapse of the Soviet Union, SASO became FMSO. Over the next decade and a half the organization's focus shifted with the Post-Cold War environment and emergence of new regions of crisis and transnational threats. No small organization devoted to a single state can easily evolve into a robust organization covering the entire globe. FMSO's leadership focused on maintaining the methodology, which had sustained the organization during the Cold War and gradually built up analytical expertise and research support in critical areas. Transnational threats, narco-trafficking, international criminal organizations, and terrorism became one area of focus with a particular investment in Latin American expertise. Graham Turbiville, a FMSO senior analyst, founded and edited the journal, *Low Intensity Conflict and Law Enforcement*, which addressed these topics. A second area of focus was the new security environment in Europe and the transitions of former Communist states of Central and Eastern Europe and the successor states of the Soviet Union. A third initial area emerged out of the crisis in the Balkans. FMSO drew upon its existing expertise, drew in Yugoslav FAOs, and engaged in outreach to academic expertise in the United States and Europe. Christopher Donnelly and I collaborated in founding *European Security*, which addressed the latter two topics.

As the Post-Cold War environment gave rise to new areas of interest and new requirements, FMSO continued to evolve. With the reduction in the number of FAOs and the emergence of new and exotic areas of national interest, FMSO faced a challenge to find new sources of talented military analysts. The "luxury" of a single, primary threat had given way to a more dynamic international order, which was being recast by the forces of globalization. FMSO became part of the Center for Army Lessons Learned (CALL) but continued to follow its own research plan and its distinct methodology. FMSO analysts conducted extensive research on peace and stability operations, the Chechen War, the Revolution in Military Affairs, and Information Operations and Information Warfare. It actively supported U.S. missions in the Balkans. FMSO analysts have taken an active part in the on-going debate over asymmetric threats across the full spectrum of conflicts. In short, FMSO focused on emerging threats in a new and dynamic international security environment.

Emerging threats gave rise to the need for a repository of open source materials devoted to more remote regions and states where crises might ignite and demand that officers and actors become "instantaneous" experts. The IC's response was the creation of the World Basic Information Library (WBIL), which it entrusted to FMSO's management. The IC provided a basic taxonomy to guide the effort. FMSO began a close collaboration with the Open Source Information System (OSIS), an unclassified network established in 1994, and serving the IC with open source materials. Under the leadership of Graham

Turbiville, Karl Prinslow, and Robert E. Waller, FMSO took a unique approach to this task and enlisted Reserve Component (RC) personnel from all Services to act as the collectors. The Reservists, who were recruited from the Individual Ready Reserve (IRR) and volunteered to provide entries for WBIL, served for "points" towards retirement and were organized into special teams covering various topics.[10]

The Reservists, who now number more than 160, are part of the Joint Reserve Virtual Organization (JRVO). FMSO also found another pool of Reservists among Military Intelligence (MI) personnel waiting for clearances who could also be utilized for open source collection. As a result of this successful utilization of reserve personnel, FMSO was selected in January 2001 to manage the newly established Fort Leavenworth Joint Reserve Intelligence Center (JRIC) joining 27 other JRICs around the country. With the Global War on Terrorism (GWOT) and the decline in the available IRR pool, FMSO turned to contract support to sustain the effort, utilizing workers with disabilities from Digital Consulting and Software Services (DCSS) Ability to provide entries.[11] At present, WBIL has more than 400,000 entries. Many Reservists have proven their capacity for independent research and have made critical contributions to FMSO's production on issues relating to transnational threats, proliferation, and terrorism.

Critical changes for FMSO began as result of its deepening involvement with the Joint and Reserve Communities. In 2000, TRADOC DCSINT became the parent headquarters for FMSO, terminating its direct tie to CAC, where it remained a tenant organization under the TRADOC DCSINT and working closely with Threats. Its missions under TRADOC DCSINT are to—

- Analyze foreign dimensions of emerging operational environments (OEs) for the Army, the IC, and the Joint Community.
- Produce quality assessments and databases.
- Provide intelligence support to operations, training, and Army and Joint Transformation.
- Build productive relationships with foreign security specialists around the world.
- Base production and database development efforts on a robust Joint Reserve Component utilization program.
- Operate and staff the JRIC at Fort Leavenworth and integrate IC programs.

TRADOC DCSINT approves the annual FMSO research plan. FMSO works closely with other elements of TRADOC DCSINT in the development of the OE, the Contemporary Operational Environment (COE), and the Joint Operational Environment (JOE). FMSO supports the JOE by providing international speakers for international conferences over the last two years. With TRADOC DCSINT support, FMSO has retained a close connection to CAC. Its director serves as a member of the editorial board of *Military Review*. Its analysts support the CGSC and the SAMS and are academic advisors to CGSC Masters of Military Art and Science (MMAS) theses and SAMS monographs. FMSO's researchers contribute to the formulation of the CAC Commander's annual list of Top 28 Research Topics.[12] FMSO works closely with CAC in identifying sources of international conflict and regional instability which might prompt U.S. engagement.

Impact of the GWOT on the FMSO

The GWOT brought other changes to FMSO. Earlier in-depth research on the Soviet-Afghan War proved particularly valuable. Les Grau, the author of *The Bear Went Over the Mountain, The Other Side of the Mountain, The Soviet-Afghan War* and 29 related articles, found himself very much in demand with senior headquarters and deploying units. In 2004, General John Abizaid, named Mr. Grau a U.S. CENTCOM Fellow. *The Other Side of the Mountain*, an account of the Soviet-Afghan War from the Mujahedin side by Grau and Ali Jalali, later Minister of Internal Affairs of Afghanistan, remains popular with those deploying to the theater. Mr. Grau heads a team of civilians and Reservists devoted to research on the Middle East and Central Asia.

In the fall of 2001, close cooperation with Joint Forces Command (JFCOM) led to the creation of a Joint Reserve Team tasked with addressing issues of Homeland Defense. This team evolved into the Northern Command (NORTHCOM) J2 Detachment at the Fort Leavenworth JRIC. FMSO also undertook on its own initiative, the creation of its Mexico Southwest and Canada Border Team. The team, composed of one civilian analyst and four reservists, produces two periodicals: The *Mexico Newsbriefs* (five issues weekly) and the *Canada Newsbriefs* (two issues weekly). These reports are unclassified intelligence summaries of articles relevant to U.S. security, primarily aimed at the tactical level but including operational and strategic reporting. They are collected and translated from approximately 50 Mexican, Central American, and Canadian press and public information sources. The team

and the NORTHCOM detachment developed a close, cooperative arrangement around the exploitation of open source information. NORTHCOM appreciated the advantages derived from the close association between its detachment and the FMSO analysts and assisted in the relocation and expansion of the Fort Leavenworth JRIC into its new, three-story facility with enhanced connectivity, thanks to the support of the Joint Reserve Intelligence Program (JRIP). This expanded facility has created opportunities for more reserve intelligence units to drill at the JRIC and other agencies to locate there. Thanks to the team's efforts, FMSO has also forged productive partnerships in the area of OSINT with the Foreign Broadcast Information Service (FBIS)—now the Open Source Center—and the Border Patrol's Field Intelligence Center (BORFIC). Recognizing the need to train personnel in open source methodology, FMSO in conjunction with the NORTHCOM J2 Detachment developed the Open Source Intelligence Research and Analysis (OSIRA) course. FMSO has also supported the National Guard Bureau's training effort in the same area.

Two other areas have enjoyed rapid growth over the last few years. FMSO's traditional focus on Latin America has taken on new direction with the application of a global information system (GIS) to support digital database development. Dr. Geoffrey Demarest has been particularly active in applying multiple layers of digitized data to the study of criminality and insurgency and incorporating property data into his analytical efforts. The intent is to use the GIS project on Colombia as a test bed for more general application into other regions of conflict. Dr. Demarest is also in the process of founding a scholarly journal, *Ibero-American Security*, the first issue of which will include papers published at a recent conference on Latin American security held in Colombia. FMSO provides foreign language news monitoring and Internet monitoring service on U.S.–Mexico border issues and on Venezuela-Colombia border issues. FMSO funds and guides extensive unclassified research on violence in Colombia as well as a major cultural geography study in Mexico. FMSO identifies threats to U.S. security emerging from the region and plans unclassified approaches to understanding those threats.

The second area has been the development of a FMSO research program on China. Mr. Tim Thomas, who has spearheaded FMSO's work on Information Operations (IO), published a collection of essays on Chinese IO under the title *Dragon Bytes* in 2004. A second volume devoted to Chinese, Russian and other approaches to IO will appear shortly under the title *Cyber Silhouettes*. In August 2005, FMSO hosted a conference on Chinese views of Central Asia. The proceedings of that conference should appear shortly. FMSO and the Asian Security Detachment, located at Camp Zama, Japan, and sharing a long-term commitment to OSINT, are looking for ways to engage in closer collaboration and mutual support. In addition to these new areas of study, FMSO continues to address Russia and other Eurasian countries. A major focus remains the conflict in Chechnya. FMSO recently began production of the unclassified Russian Defense and Security Watch, an Internet publication available on a weekly basis on OSIS.

FMSO's Future: Building on the Past to Meet New Challenges

Over the last several years FMSO has enjoyed sustained support from Congress, the JRIP, and the DA G2, who have seen value in its open source efforts. The OUSD(I) noted several areas of FMSO "best practice" in OSINT. INTELINK gave FMSO its annual award as the best website on OSIS. Recently, Representative Rob Simmons, Chairman of the House Subcommittee on Intelligence, Information-Sharing and Terrorism Risk, invited FMSO, OSIS, and FBIS to participate in a Capitol Hill fair on OSINT. FMSO is actively involved in the process of reviewing the initial draft of **FMI 2-22.9, Open Source Intelligence**, which is intended to be the Army's basic guide to OSINT and will be the first such service level publication.

FMSO benefits from the engaged leadership of TRADOC DCSINT. The TRADOC DCSINT's guidance regarding FMSO's organizational culture and mandate has eleven points:

1. FMSO is to act as a bridge between the worlds of intelligence and academe in the search for knowledge.

2. FMSO's contribution to the body of security-useable knowledge must show a valuable return on investment.

3. FMSO is to support the main effort of the U.S. military, but should not lose sight of its mandate to look away from the herd and over the horizon, to be vigilant of new threats and sensitive to the certainty of surprise.

4. FMSO should address not only threats but also the business and science of OSINT. It is a Research and Development (R&D) shop for best practices and new opportunities for security-relevant scholarship.

5. FMSO's focus is beyond the borders of the U.S., and so it must maintain competence in foreign languages and

culture, remain in direct contact with and among foreigners, and is to be familiar with their ideas and work.

6. FMSO can assist current intelligence surge requirements, but its vision is fixed on mid- and long-term trends and developments.

7. FMSO should not be in the business of advising on the organization or method of U.S. forces, but its unique perspectives on the OE and on foreign experiences call on it to write about tactics, operational art, and strategy as informed observers regarding concepts and experiences of our potential opposition whether insurgents or conventional armed forces.

8. FMSO is to capture and report allied foreign lessons-learned and foreign perceptions regarding U.S. policies and actions.

9. As the FMSO mission grows, it must maintain information security even as it works in an unclassified world.

10. FMSO should participate in the development and training of future unclassified intelligence analysts.

11. FMSO needs to manage its growth to ensure its matrix culture by effective networking, which will involve a wide range of associations and cooperation.

In accomplishing these tasks, FMSO will deliver a range of products to its consumers in the Army, Joint, Intelligence, inter-governmental, and inter-agency communities. These will include foundation knowledge (including basic infrastructure, institutional and cultural data); shaping information (including more specific military, cultural and legal data, such as property ownership, family and business associations, legal and institutional structure, religion and religious leadership, opinion and predilection surveying, biographic and historical items); situational data (including recent history and event geography and daily monitoring of some areas); and complex analyses (including its mid- and long-range studies on security-related topics.) The goal is to make this web of products valuable to a wide range of consumers. FMSO looks forward to working with the DA G2 Coordinator for Open Source and other Army open source centers to develop "best practices" in the application of OSINT to the creation of knowledge useful to warfighters.

Endnotes

1. Intelligence Reform and Terrorism Prevention Act, Public Law 108-458 December 17, 2004, Sec. 1012 Revised Definition of National Intelligence, http://travel.state.gov/pdf/irtpa2004.pdf accessed 4 October 2005.

2. Ibid., Sec. 1052 Open Source Intelligence, Sense of Congress, http://travel.state.gov/pdf/irtpa2004.pdf accessed 4 October 2005.

3. Craig Manley, "Managing Army Open Source Activities," *Military Intelligence Professional Bulletin*, 31, no. 4, (2005): 5-6.

4. "A Consumer's Guide to Intelligence," CIA (Office of Public Affairs), Washington, DC, 1999), p. vii.

5. Robin W. Winks, *Cloak and Gown: Scholars in the Secret War, 1939-1961* (New York: William Morrow, 1987), 456.

6. Michael Warner, "Wanted: A Definition of 'Intelligence'," http://www.cia.gov/csi/studies/vol46no3/article02.html accessed 4 October 2005.

7. The author wishes to thank Ms Karen Gaffin, a former FMSO intern, for the research on "The Foreign Military Studies Office: An Institutional History," which made possible the writing of this section of this article.

8. For access to these publications consult Foreign Military Studies Office, *Military Experience and Assessments from the Soviet Union and the Cold War Period*, http://fmso.leavenworth.army.mil/products.htm#MilEx accessed 10 October 2005.

9. *The Journal of Slavic Military Studies* was originally titled *The Journal of Soviet Military Studies*. The change of names reflected a broadening of interest to the militaries of the Post-Communist states of Central and Eastern Europe and those of the successor states to the Soviet Union.

10. Graham H. Turbiville Jr., Karl E. Prinslow, and Robert E. Waller, "Assessing Emerging Threats Through Open Sources," *Military Review*, September/October (1999), 70.

11. For more on the DCSS Ability program in support of the WBIL see: Matt Stearns, "Bill gives Boost to Disabled Workers," *The Kansas City Star*," 8 October 2005 at http://www.kansas.com/mld/kansas/news/state/12850405.htm accessed 10 October 2005.

12. For an examination of FMSO's role in CAC research and publications see: "Combined Arms Center Annual Research Index–2004," A special issue of *Military Review*, 2005.

Dr. Jacob W. Kipp is Director, FMSO, Fort Leavenworth, Kansas. He received his BS from Shippensburg State College, Pennsylvania and his MA and PhD in History from Pennsylvania State University. From 1971 to 1985 he taught Russian and Military History at Kansas State University. In 1986, Dr. Kipp joined the SASO as a senior military analyst, and in 2003 he became director of FMSO. He has published extensively on Soviet and Russian military history and affairs.

The World Basic Information Library Program

by Karl Prinslow

The World Basic Information Library (WBIL) Program enables Reserve Component (RC) personnel of all services, military specialties and ranks to perform research in support of the Intelligence Community (IC) and military command requirements through telecommuting—working at a time and place of their choosing. The WBIL Program was conceived in 1996 by Mr. Ed Waller then of the IC Open Source Program Office (COSPO) which developed and proved the concept, and then asked the Foreign Military Studies Office (FMSO) to manage the personnel, production, and telecommunications architecture. The founding premise was to better engage and utilize the civilian acquired skills of members of the Reserve Component (RC), especially members of the Individual Ready Reserve (IRR), by engaging them regardless of branch of service, military skills, rank or specialty, in research that supports the IC's requirements. Since its inception the WBIL program has been and remains a joint program with participants from all military services, and presently has RC, Active Component (AC), and retiree members participating as well as a group of contracted researchers—all supporting IC and unit requirements.

The ability to perform this work requires only that one have access to a computer with Internet access. All other required materials and software are provided by the FMSO office in conjunction with the Intelink Management Office which provides access to the Open Source Information System (OSIS) network. Research, collection, and archiving documents via the WBIL program are done at a time and place of the individual's choosing. That can be from a Reserve center, the individual's home or place of work, or at a Joint Reserve Intelligence Center (JRIC). The Internet is a means of contributing researched material to the WBIL, as well as for accessing the Library. The Internet is only one source of information to support the IC requirements. As long as source material can be converted to an electronic format it can be archived into the WBIL. The Internet is a principal source for the WBIL program only because of its ease in accessing and archiving.

The WBIL is hosted on the OSIS network and replicated on the Secure Internet Protocol Router Network (SIPRNET) and the Joint Worlddwide Intelligence Communciations System (JWICS). To access the OSIS virtual private network (VPN) one requests an account from the unit's "OSIS Trusted Agent" or directly from the IMO/OSIS [accounts@intelink.gov], configures the computer, and then logs on. For personnel working in the WBIL program the FMSO provides initial training material to walk a person through the process of getting OSIS access, OS information research, use of the Pathfinder software, and the methods and standards for archiving material into the WBIL. More advanced training is provided by the Open Source Information Research and Analysis (OSIRA) course described below.

The WBIL program researchers address requirements that are based upon a "sanitized" or unclassified version of the IC's requirements. Subject areas range from anthropology and culture to economics, politics, government, military, biographies, and science and technology as well as all of the emerging or transnational threats such as terrorism, drug trafficking, and information operations. Additionally, many commands and agencies make specific requests of the WBIL Program for information to support their requirements which they are not able to fulfill due to a lack of personnel or competing priorities.

The WBIL program uses intuitive and highly "user friendly" commercial-off-the-shelf (COTS) software to collect, catalog, and archive source documents in their entirety, thus the use of the term "library" rather than database or portal. In order to ensure that the source document remains accessible to the analyst, the WBIL archives the full original

document—text, imagery, sound and video—that addresses the requirement. In that way although the original Internet website may disappear, the WBIL will retain the information for perpetual use by the IC.

An individual, whether in an intelligence organization or not, accesses the WBIL by using the Pathfinder analytic suite of software. This version of Pathfinder is hosted by the FMSO on its OSIS website and is replicated on SIPRNET and JWICS by the Ground Intelligence Support Activity (GISA) and National Ground Intelligence Center (NGIC). Pathfinder permits the user to not only search and retrieve source material but also to support their analytical interests via tools such as map plotting geo-referenced materials, and conduct link analysis, establish personal databases, and perform temporal and matrix analyses. For the uncleared person this utilization of Pathfinder is an additional training benefit in preparation for doing additional future work on "the high side."

The WBIL Program Benefits the RC Community

The benefits for RC individuals working in the WBIL program are the opportunity to serve in a valued and valuable manner while earning their required Reserve drill points, contributing to their unit's mission, and having the ability to choose when and where to perform that valuable work. The individual will train on and use the tools and systems of the IC. Additionally, military members can learn about their unit's area of responsibility, use their foreign language abilities, and contribute to the overall unit mission success.

Those currently awaiting their security clearances now have a unique opportunity to participate in an unclassified program that can support their commands as well as prepare them for their "high side" missions. Individuals who are pending security clearances are a valuable resource, often trained in all aspects of their job and fully capable of performing high quality intelligence support work, albeit in an unclassified workspace. They can provide the OS component of a unit's all-source intelligence production. The WBIL Program provides a means by which any military member working from literally anywhere in the world can support his or her unit mission by performing unclassified or OS research and analysis in support of the unit's missions. The Army's Active Component and other services can also utilize the WBIL program to engage their personnel who are awaiting security clearances through unclassified research to support unit missions.

The units benefit by improved retention, recruitment, and mission success. By ensuring new personnel a valued position and contribution to the unit's mission, the unit can more successfully recruit individuals with valuable civilian and military acquired skills and eliminate the distraction and demoralizing effects of a slow security clearance process. A Reserve unit can use working under the auspices of the WBIL as a retention tool by giving meaningful and valuable work to unit members who otherwise feel left out of the unit's classified work. Additionally, remote or telecommuting work under the authorization of Rescheduled Training (RST) for Reserve members has been used as a means of retaining a soldier who is losing interest in Reserve service due to the requirement to travel to distant drilling sites. Lastly, the unit is also able to support its mission using a larger population of skilled and experienced personnel who are in the IRR and working on WBIL program standing requirements or those specifically requested by the unit. While IRR personnel are not assigned to a unit, they are available to support a unit's requirements.

Reserve Training and Research Options

The Army Reserve MIAD Program

The Military Intelligence Augmentation Detachment (MIAD) program is a means by which the Army Reserve allows MI soldiers to drill remotely from their assigned unit, thus saving the resources of time and money required to travel. The MIAD program integrates the WBIL program as a means of performing this remotely located service and doing so in a manner that can directly support their unit's mission while working in their Military Occupational Specialty in support of intelligence requirements and using intelligence tools and systems. The Military Intelligence Readiness Command (MIRC) commands all Army Reserve MI units and fully supports this manner of expanded service opportunity.

The OSIRA Course

In 2003, a multi-service detachment working with the FMSO in support of the Homeland Defense Directorate of the U.S. Joint Forces Command recognized a need for more comprehensive training. The result was the development of the OS Information Research and Analysis (OSIRA) Course. This four and one-half day course provides instruction and practical exercises on the conduct of OS research, collection and utilization of the Pathfinder search and analytic

software suite used by the IC. Additionally it instructs on topics of Intelligence Oversight, Internet research, psychology of OS Analysis, commercial Imagery, and other topics. The OSIRA Course is conducted monthly by the FMSO at the JRIC, Fort Leavenworth. The National Guard Bureau also conducts the OSIRA course with additional modules focusing on Homeland Defense.

Reach Language Support Program (RLSP).

Linguists who are awaiting a security clearance can focus their research in the WBIL program on foreign language material, both written and audio-video, thus sharpening their linguistic skills. The WBIL library archives gists or abstracts of the foreign language material along with the full text of the source document so that a researcher can get a full translation if needed at a later date. As always, a participant's work should be in support of the unit's mission requirements, otherwise the WBIL program production managers will add research topics.

If an individual, with or without a security clearance, wants to solely perform full translation work, the RLSP of the NGIC is available for this purpose, and also supports remote working. The RLSP utilizes the linguist's skills to translate foreign language documents. These translated documents are archived in the IC's Harmony databases and if unclassified, are also archived in the WBIL in order to increase accessibility on unclassified systems using the Pathfinder tools. (See the article on the RLSP in this issue of MIPB for more details.)

Conclusion

Soldiers, with or without a security clearance, who want to support national intelligence requirements have a means to do so at a time and place of their choosing through the WBIL program. Unit commanders can capitalize on the same program to enhance their unit mission success by more fully incorporating OS sources of information in their all-source production, and by capitalizing on civilian acquired skills and expertise of personnel who are not in their units, or maybe not even officially in the Intelligence field. It is almost trite to say that personnel are our most valuable resource; however, it is true. The WBIL Program provides a unique means by which the military can substantially enhance its productivity, retention, and recruitment of personnel supporting intelligence requirements.

Karl Prinslow is the FMSO's WBIL Program Manager and Site Manager of the JRIC at Fort Leavenworth. He served as a U.S. Army Infantry officer and Sub-Sahara Africa Foreign Area officer with assignments ranging from platoon leader to battalion and brigade operations officer to Defense Attache and Security Assistance Officer in numerous African countries. Mr. Prinslow retired from the U.S. Army in September 2000.

Points of Contact:

WBIL Program

Karl Prinslow, karl.prinslow@leavenworth.army.mil, 913-684-5963

Operations and Training: MAJ Shawn Carpenter, wbilops@leavenworth.army.mil, 913-684-5962

Administration: MSG Michael Keltner, wbiladmin@leavenworth.army.mil 913-684-5963

OSIS

Mr. Ed Waller, rew@center.osis.gov, 703-983-5380

OSIRA Course

MAJ Shawn Carpenter, wbilops@leavenworth.army.mil, 913-684-5962

CTA1 Kristin Delfs, krsitin.delfs@leavenworth.army.mil, 913-684-5977

RLSP

Mr. Dennis Johnson, Dennis.F.Johnson1@us.army.mil, 801-523-4300

U.S. Navy

LCDR Cindy Hurst, churst@center.osis.gov

Intelligence Philatelic Vignettes

A Non-Existent Yeshiva (Jewish Religious School) in the Service of the Pre-Israel Underground Movement

by Mark Sommer

In the 1930s, the Jewish community of British-controlled Palestine joined forces to achieve independent statehood, combat Arab rioting, and provide for the general self-defense. One group, ideologically aligning itself with Ze'Ev Jabotinsky's Revisionist Movement, rejected the "Restraint" policy of the Jewish Agency's Hagana forces. The Revisionist forces carried out armed reprisals against the Arabs, and after publication of the British "White Paper" restricting Jewish immigration to Palestine from Nazi Europe, conducted sabotage activities against the British. The underground organization was known as the Irgun Zvai Leumi (Hebrew for National Military Organization) and was headed by Israel's late Prime Minister Menachim Begin.

When Irgun members were caught, they were interned in various prison camps in Palestine (Acre, Latrun, Mazrea, and Sarafund) and in Africa (Asmara, Carthargo, and Gilgal). They were moved frequently to prevent escape, though many managed to do so.

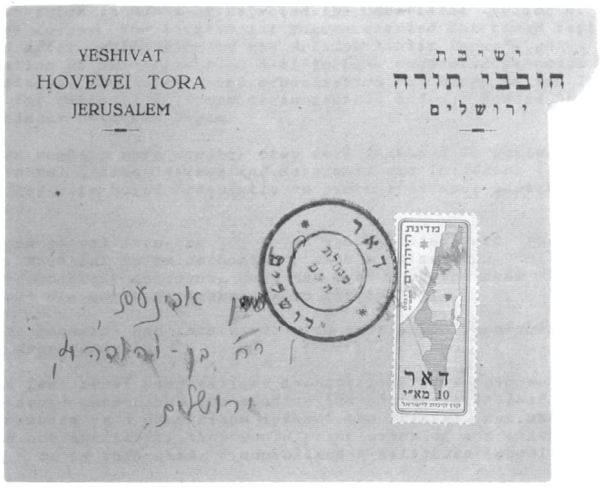
This simple postal item has led to an unusual discovery. Postmarked "May 13, 1948, Minhelet Ha'am Jerusalem" with a Palestine 10 mill stamp, it appears to be completely innocent. Only the fact that the school "Yeshivat Hovevei Tora, Jurusalem" did not exist makes it so intriguing.

After some research and interviews with people who were active at the time, the following story emerged.

The Irgun Zvai Leumi used various institutional envelopes (mostly religious to avoid detection) for sending its anti-British leaflets to local citizens and members as a subterfuge against the British. But when such genuine envelopes were not available, they would print names of non-existent institutions on blank ones – as in this case – a non-existent religious school!

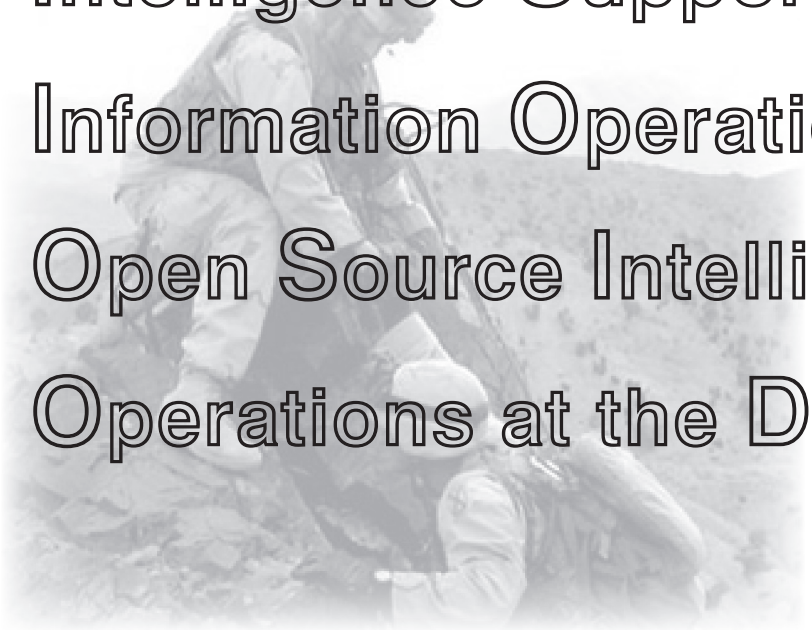
A former professor at the Hebrew University of Jerusalem, and an Irgun Zvai Leumi commander in Jerusalem, substantiated these facts and said that his wife was among those who prepared and sent these envelopes containing the leaflets.

Only a handful was ever produced and most were destroyed upon receipt due to the obvious dangers of possessing such anti-government material. It is believed that maybe only one other envelope may exist, but unless that can be confirmed, this item is truly unique.



*Mark Sommer holds a BA in Political Science from Yeshiva University and an MA in International Relations from Fairleigh Dickinson University. He teaches at Stevens Institute of Technology in the Humanities Department. His published works in the intelligence field include: "Getting the Message Through Clandestine Mail and Postage Stamps," **MIPB**, October – December, 1992 and "Undercover Addresses of World War II," **International Journal of Intelligence and Counterintelligence**, Fall 1993.*

Intelligence Support to Information Operations: Open Source Intelligence Operations at the Division Level



by Captain Laura A. Levesque

"Broadcast media and other information means can make combat operations visible to a global audience. Various actors seek to use perceptions to control and manipulate how the public views events. The enemy will exploit U.S. mistakes and failures, create disinformation based on falsehoods, and use propaganda to sway the local population to support their cause, to alienate world opinion, and to influence US public opinion. Media coverage can affect U.S. political decisionmaking, internal opinion, or the sensitivities of multinational members."— FM 2-0, Intelligence, 1-84.

Critical to understanding effects-based operations and defeating a designing enemy during counterinsurgency operations is an understanding of the information environment. The 10th Mountain Division (LI) G2 developed a portion of its Mission Essential Task List (METL) to gain that understanding by focusing intelligence support to "Provide Intelligence Support to Effects" It is a task that is critical to Stability and Reconstruction Operations.

According to **FM 7-15, The Army Universal Task List** *Army Tactical Task (ART) 1.4.2, Provide Intelligence Support to Information Operations (IO)*, the Intelligence Battle Operating System (IBOS) is responsible for providing intelligence support to effects. The three subtasks are—

- ART 1.4.2.1, *Provide Intelligence Support to Offensive IO*. ***"Offensive IO degrades an adversary's will to resist and ability to fight while simultaneously denying him relevant friendly force information."***
- ART 1.4.2.2, *Provide Intelligence Support to Defensive IO*. ***"Defensive IO protects friendly information and C² systems. Information superiority means commanders receive accurate and timely information that enables them to make better decisions and act faster than their adversaries."***
- ART 1.4.2.3, *Provide Intelligence Support to Activities Related to IO*.

The Light Infantry Division Modified Table of Organization and Equipment (MTOE/OTOE) does not appropriately address the intelligence requirement with requisite analytical support to accomplish the intelligence support to IO tasks. As a result of thorough mission and troop-to-task assessment, the 10th Mountain Division (LI) G2 identified the need for dedicated intelligence support to IO. This led to the creation of the G2 Intelligence Support to Information Operations (ISIO) cell—directly supporting the Division IO section with the G2 Analysis and Control Element (ACE). Initially, the ISIO cell consisted of one captain, All Source Intelligence Officer (35D)—dual-hatted as the G2 Targeting OIC, three Intelligence Analysts (one 96B40 and two 96B10s).

We structured the ISIO cell to collect and process data and information to support Civil Affairs Opera-

tions (CMO), Psychological Operations (PSYOP), Electronic Warfare (EW) operations, and Computer Network Exploitation (CNE) operations. Our goal was to have the capability to fuse all of this information with current and future enemy intentions and provide awareness of the effects of our IO Battle Damage Assessment (BDA) in order to provide the commanders with dominant battle space awareness. During the process of developing an IO Intelligence Preparation of the Environment and leveraging PMESII (political, military, economic, social, information, and infrastructure) to evaluate the operational environment, the requirement emerged for a separate Open Source Intelligence (OSINT) analysis cell that would be dedicated to collection and analysis of all OS media. The newly identified requirement for OSINT was to support indications and warnings; assess the intention of insurgents; host nation political environment, coalition political environment; and to determine IO BDA. The end state is to give a holistic picture through collection and analysis of OS media, to include news reports, articles, transcripts of radio broadcasts, and other media within the relevant area of responsibility (AOR).

OSINT operations also allow analysts the ability to gain an understanding of how the media provides useful information to the enemy. By tracking what information is being released through OS about U.S. and Coalition operations, the analysts can anticipate what information the enemy is exposed to and how they may exploit any information in their operations. Negative media that is released is used by the enemy in their propaganda operations against ongoing operations and U.S. and Coalition forces.

"The media's use of real-time technology affects public opinion, both in the US and abroad, and alters the conduct and perceived legitimacy of military operations. The adaptive thinking adversary will often seek to exploit the information environment in an effort to counter, weaken, and defeat the US. Information warfare will be directed against the US and US interests. While the level of sophistication of such attacks may vary, they nonetheless will take place and over time will take their toll."

In order to create an OSINT cell, also not documented on a Light Infantry Division MTOE, we split the ISIO cell and sourced it with one captain (35D), one Signals Intelligence Analyst (98C40) with limited IO experience, and four 96B10s, distributing two of the 96B10s to focus solely on OSINT.

The OSINT cell currently generates two products. The first is an unclassified daily news summary that is divided into four subject areas: media (local and regional political news and internal activities) relating to Afghanistan; national U.S. media; CONUS force protection and situational understanding (ranging from natural disasters to possible terrorist activities), and international media. The purpose is to collect all unclassified media and combine it into one product that can be referenced to provide information and situational awareness for activities that can affect current or future operations.

The second product is the 10th Mountain Division's (LI) *Mountain Sentinel*. The focus areas for the *Sentinel* are local, regional, and international media relating to activities or policies which are internal to or affect Afghanistan. Currently the scope of media is limited due to location and access to the media materials. The objective is to incorporate web sites, blogs, local gossip, radio broadcasts, mosque assessments, local newsletters, insurgent propaganda, and all other media produced in the AOR. The purpose is to collect from any medium that can reveal indications or intentions that may have an affect on PMESII in Afghanistan. The OSINT cell further develops the *Mountain Sentinel* to include an analytical assessment of the information and provide a monthly overall assessment of Afghanistan's media climate. The OSINT cell publishes *Mountain Sentinel* weekly during garrison activities prior to deployment to Operation ENDURING FREEDOM (OEF VII), and daily in deployed operations. The *Sentinel* is used as a "tipper" to cue other assets for possible operations or changes that may affect the area of operations (AO).

In the planning process, the *Sentinel*, when fused with population viewpoints in a given area, can be used as a subject analysis tool to characterize how operations are currently, or may in the future, positively or negatively affect local sentiments. It is used as one of the ways to measure the effectiveness of the IO and PSYOP campaigns. The finished intelligence product also supports the assessment of campaign plan objectives. The OSINT cell works closely with the division Public Affairs Office and the division PSYOP cell to collaborate on media sources and content and to confirm source assessments.

Challenges of personnel and collection capability remain, but can be mitigated upon our arrival in theater. A potential solution is to hire contractors, fluent in the predominant Afghan languages, to read and translate media from within the AOR. PSYOPs would also prove to be an asset in the collection of media in remote areas where we would not otherwise have access. By understanding the battlespace, our Every Soldier is a Sensor (ES2) concept leverages every soldier sensor to collect OS media such as flyers, posters, and graffiti that could contain relevant information. Once the materials are gathered, translated, and analyzed, they can be used as a part of the overall analysis of the complete media environment.

Although the OSINT cell currently faces challenges with limitations in variety of information, once in theater we can identify resources and information to be used in addition to online media sources. The use of media that has been collected from within Afghanistan will allow the analysts to create a more complete picture and provide depth in local, regional, and national media analysis.

Endnotes

1. **FM 7-15**, **The Army Universal Task List**, ART 1.4, 1-1.

2. **FM 2-0**, **Intelligence**, 1-75.

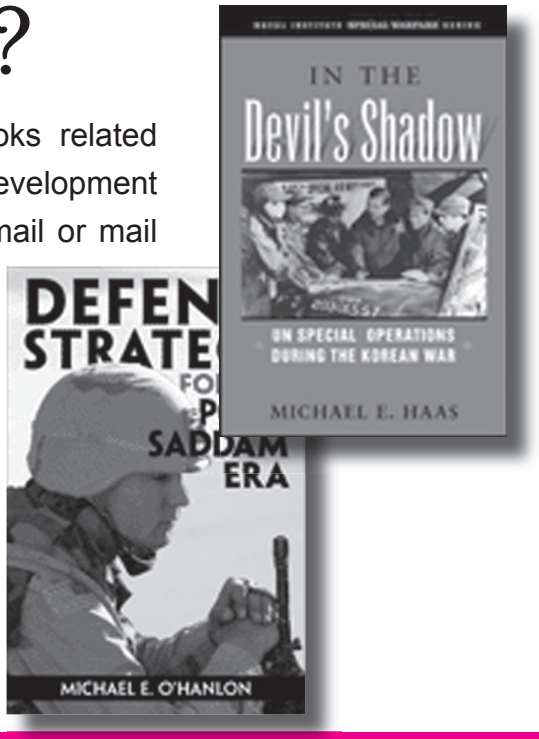
3. **FM 2-0**, 1-75.

4. **FM 2-0**, 1-74

Captain Laura A. Levesque is currently serving in the 10th Mountain Division (LI) at Fort Drum, New York. She is the division's G2 Information Operations Intelligence officer. Her previous assignments include division Intelligence Targeting Officer, HHOC Executive Officer, 110th Military Intelligence Battalion, and S2, 210th Forward Support Battalion.

Read Any Good Books Lately?

We weclome reviews of books related to intelligence professional development or military history. Please E-mail or mail your book reviews with your phone number, address, the title, author, publisher's address (listed on the book's copyright page). Please send your reviews to mipb@hua.army.mil or mail them to ATTN: ATZS-FDT-M USAIC&Fort Huachuca, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017.



Non-Governmental and Inter-Governmental Organizations

by Carol J. Koenig

Introduction

Non-Governmental Organizations (NGOs) and Inter-Governmental Organizations (IGOs) are an important part of open source information for any organization. Using NGOs and IGOs to obtain open source information involves consideration of the vast diversity of these organizations and careful evaluation of the information obtained. Some generalities in this article may not apply in all cases.

Although the World Bank has described NGOs and IGOs as "civil societies," the designations NGO and IGO seem to better describe what these organizations are and do. The IGOs are formally created by two or more usually legally recognized governments that agree upon a mutual need, plan an organization to meet that need, and sign a formal agreement to constitute an organization and fund its operations. IGOs therefore have international legal status, and their employees technically have diplomatic status that may or may not offer safe haven in troubled areas of the world (e.g., the 2003 Baghdad United Nations (UN) headquarters bombing and death of the UN representative in Iraq.

Founding countries usually fund an organization's budget, administrative structure and guiding board, establish a central organization office, and hire employees. IGOs generally fall into two categories: global and regional. Examples of the global IGOs are the UN and its many affiliated agencies, Interpol, the World Commission on Dams, the International Organization for Standardization, and the International Water Association. Examples of regional IGOs are the Nile Basin Initiative, the Organization of Arab Petroleum Exporting Countries (OAPEC), the Nubian Sandstone Aquifer System, and the Asia Pacific Network Information Center.

Unlike IGOs, the NGOs are usually private, not-for-profit organizations that seek social change through the use of political influence. NGO activities are usually smaller in scale than those of the IGOs and have deeper local roots with field-based expertise. Pamela Aall divides NGOs into four types: humanitarian, human rights based, society and democracy building, and conflict resolution.[1] Examples of each follow:

Humanitarian. American Near East Refugee Aid, SOS Attentats, the Center of Excellence in Disaster Management, and Humanitarian Assistance, Humanitarianinfo, Interaction.

Human Rights Based. The World Organization Against Torture, the Palestinian Human Rights Monitoring Group, Physicians for Human Rights, the Unrepresented Nations and Peoples Organization.

Society and Democracy Building. The Coalition to Stop the Use of Child Soldiers, Opendemocracy, the Campaign Against Arms Trade, the "International Institute for Democracy and Electoral Assistance.

Conflict Resolution. War-torn Societies International, the Carnegie Endowment for International Peace, the Institute of Peace and Conflict Studies, the Stockholm International Peace Research Institute.

Open Source Research on NGOs and IGOs

Most NGO and IGO web sites have .org or .net, and occasionally .int domains. NGO and IGO web sites located in foreign countries usually contain a .org or a .net somewhere in the universal resource locator (URL) before the final country domain designation. Some of the best web starting points for NGO and IGO research are at a .com site such as *Periscope's* daily email, any major world newspaper, and the usual television news sites. The current event reports of these sources often include mention of some NGO and IGO groups operating in the area of interest. A researcher can then go to the web site of a named group to read posted reports, journals, pleas for assistance, letters, and articles. These

web sites often have links to more web sites (usually NGO or IGO and often even more esoteric) with related information. Educational web sites are also good places to find references to NGO and IGO web sites. The idealism of college students encourages them to link their university server .edu web site to web sites of groups that are working to stop wars, promote democracy, save children, aid victims, feed refugees, combat AIDS, and stop global warming.

Blogs, particularly those free-wheeling travel blogs created by sandal-footed backpackers in worldwide Internet cafes located in Third World countries, often contain references to NGOs and IGOs working in the immediate area. Even, the UN maintains a new blog on UN information and web sites at *UNBlog*.

NGOs and IGOs have experienced exponential growth in recent years. The World Bank estimates these "civil societies" to number between 6,000 and 30,000, but an exact number is impossible to pin down due to their extremely fluid nature and usually non-coordinated existence. NGO and IGO web sites are usually very good places to find statistics, but they must be carefully evaluated because all NGOs and IGOs have agendas. The UN agendum is quite different from that of the OAPEC, for example, but the agenda are there and are far too often influenced by the entity funding the group (i.e., a group of Arab businessmen, a church, a military dictator, a think-tank, the Chinese government, etc.).

The quality of NGO and IGO web sites differs. Some are technologically adept and sophisticated at promoting their message (e.g., the Israeli Information Center for Human Rights in the Occupied Territories). Some web sites with simple beginnings (e.g., the Albanian National Army of Montenegro) suddenly die for reasons such as failure of the country's electrical grid infrastructure, lack of trained information technology workers, or the cause itself is overcome by events.

Some causes, however, are continuous. Church (NGO) web sites are examples that remain a very good source for worldwide information. Especially good are the Religious Society of Friends (Quakers), various Mennonite groups, and the Church of Jesus Christ of Latter Day Saints (Mormon) sites. Some of their missionaries serve in places no one else goes, and their representatives are often admitted into conflict areas. Church mission reports usually provide excellent on-the-ground current information.

Although not NGOs or IGOs per se, international conferences and commercial exhibitions often set up a .org web site to present their proceedings and advertise their wares before printed materials are distributed. Often no plans are made for post-event web site operations, so these conference and exhibition web sites sometimes remain active for several years, providing information not readily available from the participants' current web sites with webmasters on the organization's payroll.

Searching international web sites is obviously easier when one has access to foreign language keyboards and knowledge of the target country's language. When searching only in English, one should try all spelling variants (armor, armour; Ivory Coast, Cote d'Ivoire).

Another aspect of worldwide webbing is deciding how much (if at all) a researcher wants to allow a potential adversary knowledge of who is searching its web site and the country from which it is being searched. There are many commercial-off-the-shelf (COTS) anonymizers available that provide operational security. This anonymous Internet searching can allow access to terrorist web sites that present a very different face to a .1b-domained searcher than to a .mil-domained searcher.

A researcher should also consider unusual Internet web sites and think creatively. For example, search country-specific speleological web sites for information about terrorist hideouts; search a country's civil engineer society web sites for copies of infrastructure reports often done at the local government's request and guidance. And follow the money. Search the web sites of money-granting institutions for reports on road building in central Asian republics or information on electrical infrastructure upgrades in war-torn countries or new developments in mine detecting equipment.

The main challenge of gathering NGO and IGO open source information is to comprehend the immense diversity of these organizations and to find ones that are useful to your organization.

Other suggested starting points are:

- CBS News Disaster Links at http://www.cbsnews.com/digitaldan/disaster/disasters.shtml
- The U.S. Department of State. United Nations and Other International Organizations: Postal Addresses, Internet Sites, and Contacts at http://www.state.gov/p/io/empl/11078.htm
- American Library Association. Government Documents Round Table International Documents Task Force at http://www.library.uiuc.edu/doc/idtf/home.htm.

- ❑ Official Web Site Locator for the United Nations System of Organizations: Alphabetic Index of Web sites of the United Nations System of Organizations at http://www.unsystem.org/en/frames.alphabetic.index.en.htm
- ❑ United Nations Publications. (annual with seasonal updates, or online) at http://unp.un.org/
- ❑ Duke University. Perkins Library. Public Documents and Maps Dept.
- ❑ Non Governmental Organizations Research Guide at http://docs.lib.duke.edu/igo/guides/ngo/
- ❑ World Bank Group. The World Bank and Civil Society at http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/CSO/0,,pagePK:220469~theSitePK:228717,00.html
- ❑ Directory of Development Organizations. Lists over 43,000 organizations divided geographically and further subdivided into nine categories at http://www.devdir.org/
- ❑ Idealist.org: Action Without Borders. See "Organizations" section of over 48,000 listings that can be searched by name or by area of the world at http://idealist.org/
- ❑ Union of International Associations. Hardcover edition of the Yearbook of International Associations: Guide to global civil society networks. Available online by subscription only; most libraries have a CD or hard-copy edition at http://www.uia.org/organizations/volall.php

Suggested Reading

- ❑ Jonathan P. Doh and Hildy Teegen, *Globalization and NGOs: Transforming Business, Government and Society* (Westport: Praeger Publishers, 2003).
- ❑ Craig Warkentin, *Reshaping World Politics: NGOs, the Internet, and Global Civil Society* (Lanham: Rowman & Littlefield Publishers, Inc., 2001).

Endnotes

1. Pamela Aall, Daniel Miltenberger and Thomas Weiss, 2000. *Guide to IGOs, NGOs, and the Military in Peace and Relief Operations*. (Washington, D.C.: United States Institute of Peace Press, 2000).

The author, Carol Koenig, currently at the National Ground Intelligence Center, formerly worked within academia (University of North Carolina, Chapel Hill) and for the U.S. Army. She holds a BA from the University of Kentucky in European History, a BS from the University of Maryland University College in Information Systems Management, an MA degree from Trinity College (Connecticut) in Ancient History, and an MS degree from the University of North Carolina at Chapel Hill in Library Science. She can be contacted at carol.koenig@us.army.mil.

Open Source—It's Everywhere, Even on INTELINK central

by Sally S. Sanford and Ann L. Miller

Open source information is unclassified information that is available on the Internet at public libraries, on the television, and in newspapers and magazines and other media formats. The Intelligence Community's (IC) Intelink systems, on the Joint Worldwide Intelligence Communications System (JWICS) and Secure Internet Protocol Router Network (SIPRNET), contain a wide variety of the open source information. The intent of this article is to highlight some of these unclassified information sources available on Intelink. We hope this article will also inspire readers to investigate Intelink for their own open source information needs. Please note that information sources described in this article are current at the time of writing, but web sites and their contents are subject to change without prior notice.

The Intelink Central Homepage

There are three categories of Intelink sites with open source information: the Intelink Central homepage, unclassified sites from other intelligence agencies, and open source information accessed on classified sites. The Intelink Central homepage has more open source sites in quantity and variety than any other single web page on Intelink. The sites listed below are examples of the variety of open source information that can be reached from the Intelink Central homepage. If you don't have the Intelink Central homepage already saved in your browser, look for a link to Intelink Central on the homepages of individual agencies.

The World Factbook

The Central Intelligence Agency publishes the World Factbook annually. Countries are listed alphabetically with current definitions and statistics in various subject categories: geography (including maps), demographics, health, government administration, political structure, diplomatic and international issues, military statistics, communication and transportation networks, economics, and transnational issues.

Jane's Information Group

Jane's Information Group provides information related to worldwide military, defense, and security developments. Topics covered include force structure, trends, security, news, politics, equipment (specifications, design upgrades,

producers, end users, etc), military or defense demography and geography, charts, and images.

CNN Headline News

Audio broadcasts of recent (usually up to the last 24 hours) CNN Headline News. Audio software that can process files with an .au extension is needed for this site.

The Open Source Center, formerly known as the Foreign Broadcast Intelligence Service (FBIS)

This site contains articles and images culled from worldwide news sources and other publicly available material. Areas covered include local events, terrorism and crime, politics, environment, military actions, defense affairs, people in the news, and country issues.

Early Bird

Daily items from newspapers, periodicals, radio, and television that cover subject areas of interest to U.S. policymakers and other key personnel. Subject areas include politics, military topics, international events, economics, business, and editorials.

Economist Intelligence Unit

The Country Reports are published monthly and the Country Profiles are published annually. More that 180 countries are covered. Each Country Report provides an analysis of the current political and economic situation for that country along with trade statistics and an economic projection for the next 12 to 18 months. The Country Profile discusses social and political issues affecting each country, including a five-year statistical table of economy related data.

U.S. Special Operations Command (USSOCOM) Open Source Publications

This site contains news articles about world regions (Central and South America, Africa, Central Asia, and Pacific Rim) on subjects of crime, instability, security forces, and foreign affairs. Tribal studies include Iraq, Sudan, Pakistan, and Afghanistan border tribes. Topics in the travel studies section include transportation to, from, and within countries; money; culture; business etiquette; U.S. embassies and consulates; cyber and other available communications; city briefs, and security for women travelers.

Intelink Gazetteer

The Intelink Gazetteer, also known as the GEOnet Names Server (GNS), provides access to the National Geospatial-Intelligence Agency's (NGA) and the U.S. Board on Geographic Names' (U.S. BGN) database of foreign geographic feature names. The official repository of foreign place name decisions approved by the U.S. BGN can be found at http://earth-info.nima.mil/gns/html/bgn.html. Approximately 20,000 of the database's features are updated monthly. Geographic area of coverage for this database is worldwide, excluding the U.S. and Antarctica. For names in the U.S. and Antarctica, visit the U.S. Geological Survey (USGS) Internet site at http://www.usgs.gov/ or Geographic Names Information System (GNIS) at http://geonames.usgs.gov/.

U.S. Central Command (USCENTCOM) Foreign Media Perceptions Archive

This archive, prepared by the Coalition Intelligence Center's Open Source Intelligence Cell, is a survey by date of foreign media reporting and commentary on the continuing war on terrorism. The articles are selected as representative samples of local media views and interpretations of current events. Articles that are presented in the Foreign Media Perception are derived entirely from open sources in and around the CENTCOM area of responsibility. The "General Themes" section is a summary of the most prevalent messages and is not an endorsement of the validity of the information contained in the articles. The archive dates back to January 2005.

Tools

Some of the tools at this site are a currency converter, Periodic Table of the Elements, quadratic equation solver, calendar of international holidays and events, temperature calculator (Celsius, Fahrenheit, Kelvin, and Rankine), time zone converter, geographic converter (UTM, worldwide datums, etc.), moon phase dates, length and mass measurements, and other converters and calculators.

Maps

The Maps button, found under the Intelink Central picture of a World Map, is a link to a wealth of map and geolocator resources, most of which are unclassified. This page lists major Intelink-TS or Intelink-S map sources, with a brief description of each site and provides a link to a broader list of sites with additional maps.

Open Source Information on Unclassified Sites

Some unclassified open source sites from other intelligence agencies are not listed on the Intelink Central homepage but can be found elsewhere on Intelink.

Wireless Telecommunications Analysis (JWICS only)

This site is a repository of open source information about commercial wireless telecommunication markets, industries, and user countries worldwide.

International Trade Monitor (JWICS only)

The information on this site is somewhat dated, but it could serve as an excellent starting point for the analysis

of international trade growth and changes. The information is organized by geographical regions and countries within those regions. Information is also organized by subject areas such as Trade Blocs, World Trade Flows, Major Traders by Region, and Commodity Prices.

Open Source Information on Classified Sites

There are many classified sites on Intelink with open source information, but not all of this information is easy to find on a site's homepage. Some of the sites with open source are the following:

PORTAL (JWICS only)

PORTAL is the National Air and Space Intelligence Center's all source information repository. Information components, also known as libraries, are arranged by classification levels. There are two unclassified libraries, U-CIRC (information dates from 1960 to 1999) and DELFI (information dates from 1999 to the current year). This worldwide information is primarily about scientific and technical subjects. Users must register for access to this database.

Marine Corps Intelligence Activity Country Handbooks (JWICS and SIPRNET)

The Country Handbooks are designed for field use. The handbooks show U.S. personnel what they are likely to encounter while in the individual country. There is information on U.S. diplomatic sources, entry requirements, medical and environmental assessments, communications, geography, climate, culture, armed forces (including training and equipment), politics, government, history, economics, and threats to U.S. personnel. Maps and images are included.

Armed Forces Medical Intelligence Center (AFMIC) (JWICS and SIPRNET)

The AFMIC site provides current alerts and in-depth classified and unclassified studies on worldwide and country level health, medical, and associated environmental issues. The Medical Capabilities Overview reports, found under Global Health Systems, describe a country's capability to provide its military with medical care and support. The Infectious Disease Risk Assessments identify a country's diseases ranked by risk of exposure and outbreak among U.S. personnel. The Infectious Disease Alerts report recent significant disease outbreaks or problems. There are additional open source information documents available as this site.

Topographic Engineering Center (JWICS and SIPRNET)

Maintained by the U.S. Corps of Engineers, this site gives classified and unclassified in-depth geographic and environmental information for foreign countries. The Engineering Route Studies are country maps showing such information as ground transportation networks (road types, bridges, tunnels, sealift capable ports, railways, C-130 capable airfields, etc.), terrain descriptions, drainage, and areas of potential flooding or landslides. The Military Capabilities Studies are references for operational and tactical planners. These studies have information on a country's soil types, hydrology, and terrain conditions that affect cross-country movements, climate, vegetation, and other physical environment features. Some of the other unclassified documents available here are Water Resources assessments and Urban Tactical Planner data sets.

Joint Staff J2 Multimedia Library (JWICS and SIPRNET)

Since 1998 the library has been archiving multimedia content for use by customers throughout the IC and the Department of Defense. The effort came to prominence during Operation IRAQI FREEDOM when the rapid dissemination of relevant open source photographs and videos assisted in the bomb damage assessment process. This web site is an attempt to provide Intelink users with tailored access to timely multimedia products. In order to provide an individualized browsing experience, users must register. Users may access this web site anonymously; however, some features will not be available.

Conclusion

As is evident from this list, open source information is available on Intelink from a variety of sources. Some of this information is very easy to find, whereas other open source information sites are buried two or three layers deep within an organization's web page. Whatever the case may be, open source information is worth finding. It can provide you a wealth of information that may not be available in the classified information world.

Sally S. Sanford is a Technical Information Specialist, a member of the Research Services Team, the Training Coordinator with the Information Services Division, Information Management Directorate, National Ground Intelligence Center. Readers my contact her via email at sally.sanford@mi.army.mil and by telephone at (434)980-7621.

Ann L. Miller is a Technical Information Specialist and Team Leader of the Research Services Team, Information Services Division, Information Management Directorate, National Ground Intelligence Center. Readers may contact her via email at ann.l.miller@mi.army.mil and by telephone at (434)980-7516.

THE NATIONAL VIRTUAL TRANSLATION CENTER

by Dr. Kathleen Egan, PhD

What Is the National Virtual Translation Center?

The National Virtual Translation Center (NVTC) is a government interagency entity established by congressional mandate to provide timely and accurate translation of foreign intelligence for all elements of the Intelligence Community (IC). Our mission is not to replace, but rather to augment and supplement the foreign language capabilities present in all elements of the IC and the military.

The NVTC is developing and employing state-of-the-art technologies to broker translation services and provide the translated product in a format suitable for receipt from and dissemination to a broad IC and military customer base. Our vision is to be the trusted provider of choice for interagency translation services, while demonstrating a national virtual model.

Who are the NVTC Customers?

An NVTC customer is always a government client who has intelligence related translation needs. The NVTC strives to meet the needs of two types of customers: recurring and non-recurring. Recurring customers have large tasks for which Service level agreements are forged and ongoing work is performed over longer periods of time. Non-recurring customers are most often in need of one-time, or ad hoc, translations. As a result, the NVTC has positioned itself to respond rapidly to a wide range of request types. The NVTC business model stresses agility, flexibility, and dynamics. For those customers who have an ongoing task, the NVTC has established procedures and a concept of operations to ensure dataflow and dedicates task managers and linguists to serve the needs of those customers.

The NVTC has provided language services to 38 distinct customers from within the IC and National Security arenas in the past three years of existence. The IC has been increasingly challenged to keep pace with the growing need for translation of foreign language material. Operational experience gained over the past 3 years at the NVTC confirms the need for an interagency entity to supplement IC translation needs. The IC's 15-member agencies contain a myriad of elements and specialized centers. Each of these agencies, centers, and elements has unique language processing capabilities or needs. In FY2004 and FY2005, the customer set grew rapidly as a result of the NVTC becoming known as a translation hub for the IC. The NVTC's customer base expanded to include the many Central Intelligence Agency offices and various Department of Defense entities–the U.S. Central Command (CENTCOM), the Iraqi Survey Group (ISG), and Combined Media Processing Center-Main (CMPC-M), and others. These tasks range from critical quick turn-around responses (in a few hours from the request time to the delivery of the finished product) to ongoing high-volume tasks. In addition to the variety of customers and quantity of words requiring translation, the NVTC receives a broad range of types of documents to be processed. These come from various sources (audio, video, handwritten, typed texts), genres (formal and colloquial language documents), and levels of protection and classification (Unclassified, For Official Use Only, Secret, and Top Secret).

Examples of customer's needs range from an immediate response to a crisis such as the Indian Ocean tsunami in December 2004 to ongoing requests from Community analysts who need information support from such databases as Harmony or the Open Source Center. For the tsunami disaster relief effort, the U.S. Marine Corps sought assistance from the NVTC in translating common expressions into several languages of the tsunami-affected area. These phrases would be used while delivering humanitarian aid to the victims of the disaster. The NVTC technology team responded by

creating a website to host Sinhalese and Tamil language survival kits that NVTC operations team had acquired and translated. The website was the most expedient mode of dissemination to the Marine Corps enabling an easier coordination of effort between the deployed forces and supporting government agencies. In addition, the materials were downloaded, printed, and provided on laminated cards to the Marines deployed to relief sites. Those organizations that had access to the Internet were also supplied with the audio files that accompanied the written phrases. Support from the U.S. Department of State and the Defense Language Institute made this quick turn around a possibility by providing the needed human language resources and existing language kits. These language survival kits were also made available to international relief organizations that responded to the disaster.

Logo of the National Virtual Translation Center

Another example of a response to customer's needs is the CENTCOM Open Source Intelligence (OSINT) unit that was tasked on a daily basis with requests for information from various open sources. While they relied on FBIS.gov (now OpenSource.gov) at the time, they also needed direct access to foreign news (broadcast and online newswire and Internet sites). These resources were exploited through state-of-the-art technologies in speech to text and machine translation to determine what needed human translation. A full workflow was established between the customer and NVTC for daily requests and return of finished translations in less than 4 hours on average, depending on the length and urgency of the request.

In addition to serving individual IC components and organizations, the NVTC has become the lead translation service for customers using the Harmony database both on Joint Worldwide Intelligence Communications System (JWICS) and the Secure Protocol Router Network (SIPRNET). The NVTC provides translation of intelligence-related foreign language documents at the request of individual analysts from across the IC regardless of their agency affiliation.

The NVTC has established numerous agreements and relationships with various IC agencies to enable them to submit their data for translation. Most customers will request an account with the NVTC and after determination of the specific needs, a project plan is put together and the data is loaded in the Translators Online Network Support (TONS) system for assignment, tracking, and dissemination of the product. Funding is required to pay for translation costs.

Who are the Translators?

The NVTC has begun to identify and develop a cadre of trained, cleared, and vetted linguists who are available to meet the foreign language needs of the IC. To meet this challenge without interfering with the language needs of our partner agencies throughout the Community, the NVTC maintains a marketing campaign both on line through our public website and through various conferences to attract and retain qualified linguists in many languages and subject domains. The NVTC's web presence on the open Internet (http://www.nvtc.gov) increases our ability to recruit linguists from across the United States. The NVTC has employed over 400 linguists to meet its mission (and has vetted many more.)

The NVTC relies on the Federal Bureau of Investigation (FBI) for security clearances and testing language skills. All contract linguists must be U.S. citizens and perform services for the NVTC while in the U.S. The contract linguist must be able to obtain a Top Secret security clearance and undergo a language proficiency screening. Although many contract linguists work with unclassified materials, it is the NVTC security policy to screen linguists to ensure security of sensitive material. Since inception, the NVTC has employed over 400 contract linguists across the more than 40 languages in which the NVTC has performed work. Qualified linguists who wish to work with the NVTC are invited to check the NVTC's internet website.

Government or military personnel may work with the NVTC in coordination with their present supervisor or military chain of command. Separating or retiring civilian and military personnel are invited to contact the NVTC through our website to begin the hiring process as they approach their retirement or separation date.

How does the NVTC Operate?

The NVTC program office is in Washington, DC. However, the translators and customers working with us are everywhere in the U.S. The NVTC is virtual entity, allow-

ing translators to telecommute when performing unclassified tasks and/or in a government facility for other type of translations. All translators are vetted even for unclassified type work.

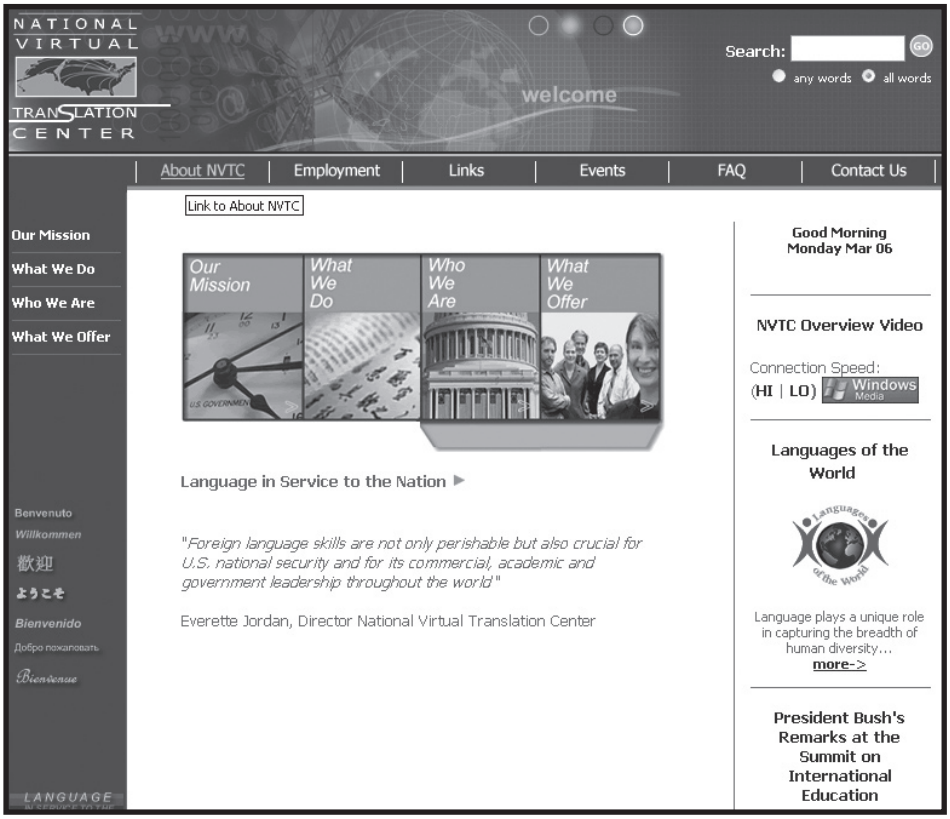
When translators working for the NVTC are assigned classified work, they are directed to a nearby facility which is certified to handle the material at the appropriate classification level. The NVTC has negotiated agreements to use facilities owned and operated by various agencies within the U.S. government to support translators distributed throughout the U.S. Such agreements allow translators who are not local to the NVTC program office in Washington, D.C., to access a secure facility (provided they have appropriate clearances), and perform work in support of the NVTC. Among the various types of facilities are FBI Field Offices, Joint Reserve Intelligence Centers, other military facilities, and academic Institutions.

The NVTC business model is designed to employ translators from any location within the U.S. With this in mind, many of the NVTC information systems, including the core translation workflow components, were designed to be used on the Open Internet in a Virtual Private Secure Network with an SSL access-controlled mechanism.

In addition to the public Internet site, the NVTC maintains informational websites on classified and unclassified Community networks (Open Source Information System (OSIS), SIPRNET, and JWICS) that are designed for customer relations, such as response to frequently asked questions and an NVTC contact page for government entities requesting accounts and more information.

The NVTC uses the IC network systems and connectivity at all levels of classification to conduct daily business. In addition, the NVTC has developed and implemented an enterprise level translation workflow management system, the TONS system, which is being examined by several other IC agencies as a model for conducting the translation business.

To learn more about the NVTC and to get your translation needs met, visit the NVTC on any of the websites www.nvtc.gov (classified or unclassified) or email Steve Grimaud, the Director of Operations at sgrimaud@nvtc.gov to discuss your unique needs and how the NVTC can serve you best. If you are interested in the technology used at NVTC, email Dr. Kathleen Egan, the Director of Technology, at kegan@nvtc.gov to gain further information.



National Virtual Translation Center Homepage.

MI Corps Hall of Fame Nominations

The Office of the Chief of Military Intelligence (OCMI) accepts nominations throughout the year for the MI Hall of Fame (HOF). Commissioned officers, warrant officers, enlisted soldiers, and civilians who have served in a U.S. Army Intelligence unit or in an intelligence position with the U.S. Army are eligible for nomination. A nominee must have made a significant contribution to MI that reflects favorably on the MI Corps.

The OCMI provides information on nomination procedures. If you wish to nominate someone, contact OCMI, Futures Directorate, U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-MI (HOF), 110 Rhea Avenue, Fort Huachuca, AZ 85613-7080, or call commercial (520) 533-1180, DSN 821-1180, or via E-mail at OCMI@hua.army.mil.

GET PUBLISHED, WIN MONEY, CONTRIBUTE TO THE CAUSE

For the 2006 General William E. DePuy Professional Military Writing Competition, Military Review seeks original essays on subjects of current concern to the U.S. Army. This contest is open to all. The Global War on Terror, evolving threats, force reform, insurgency/counterinsurgency, cultural awareness in military operations, tanks in urban combat, transitioning from combat to stability and support operations, ethical challenges in counterinsurgency, historical parallels to current operations, better ways to man the force—the possible topics are limitless. Winning papers will be carefully researched, analytically oriented critiques, proposals, or relevant case histories that show evidence of imaginative, even unconventional, thinking. Submissions should be 3,500 to 5,000 words long.

First prize is featured publication in the May-June 2006 edition of Military Review, a $500 honorarium, and a framed certificate. Second and third prizes offer publication in Military Review, a $250 honorarium, and a certificate. Honorable mention designees will be given special consideration for publication and certificates.

Essays should be submitted with an enrollment form not later than 1 April 2006 to Military Review, ATTN: Competition, 294 Grant Avenue, Fort Leavenworth, KS 66027-1254, or via email to milrevweb@leavenworth.army.mil (Subject: Competition). For a copy of the enrollment form and additional information, visit Military Review's website at http://www.leavenworth.army.mil/milrev/.

Contact and Article Submission Information

This is your magazine. We need your support by writing and submitting articles for publication.

When writing an article, select a topic relevant to the Military Intelligence community.

Articles about current operations and exercises; tactics, techniques, and procedures; and equipment and training are always welcome as are lessons learned; historical perspectives; problems and solutions; and short "quick tips" on better employment or equipment and personnel. Our goals are to spark discussion and add to the professional knowledge of the MI Corps and the Intelligence Community at large. Propose changes, describe a new theory, or dispute an existing one. Explain how your unit has broken new ground, give helpful advice on a specific topic, or discuss how new technology will change the way we operate.

When submitting articles to *MIPB*, please take the following into consideration:

- ❑ Feature articles, in most cases, should be under 3,000 words, double-spaced with normal margins without embedded graphics. Maximum length is 5,000 words.
- ❑ Be concise and maintain the active voice as much as possible.
- ❑ We cannot guarantee we will publish all submitted articles and it may take up to a year to publish some articles.
- ❑ Although ***MIPB*** is theme driven, you do not need to "write" to a theme.
- ❑ Please note that submissions become property of ***MIPB*** and may be released to other government agencies or nonprofit organizations for re-publication upon request.

What we need from you:

- ❑ A release signed by your local security officer or SSO stating that your article and any accompanying graphics and pictures are unclassified, nonsenstitive, and releasable in the public domain. Once we receive your article, we will send you a sample form to be completed by your security personnel.
- ❑ A cover letter (either hard copy or electronic) with your work or home email addresses, telephone number, and a comment stating your desire to have your article published.
- ❑ Your article in Word. Do not use special document templates.
- ❑ A Public Affairs release if your installation or unit/agency requires it. Please include that release with your submission.
- ❑ Any pictures, graphics, crests, or logos which are relevant to your topic. We need complete captions (the who, what, where, when, why, and how), photographer credits, and the author's name on photos. Please do not embed graphics or photos within the article's text; attach them as separate files such as .tif or .jpg. Please note where they should appear in the article.
- ❑ The full name of each author in the byline and a short biography for each. The biography should include the author's current duty assignment, related assignments, relevant civilian education and degrees, and any other special qualifications. Please indicate whether we can print your contact information, email address, and phone numbers with the biography.

We will edit the articles and put them in a style and format appropriate for ***MIPB***. From time to time, we will contact you during the editing process to help us ensure a quality product. Please inform us of any changes in contact information.

Send articles and graphics to MIPB@hua.army.mil or by mail on disk to:

ATTN ATZS-DCF-DM (Smith)
U.S. Army Intelligence Center and Fort Huachuca
550 Cibeque Street
Bldg. 61730, Room 124
Fort Huachuca, AZ 85613-7017

If you have any questions, please email us at MIPB@hua.army.mil or call 520.538.0956/DSN 879.0956. Our fax is 520.533.9971.

Military Intelligence Professional Bulletin
Upcoming Themes for Article Submission

Issue	Theme	Deadline
Apr-Jun 06	Cultural Awareness	15 Apr 06
Jul-Sep 06	Counterinsurgency Operations (COIN)	01 May 06
Oct-Dec 06	National Agency Support to Intelligence Operations	01 Jul 06