Open Source Information Exploitation
for
Army Force XXI

Summary

The information explosion of the 1990s and its increasingly easy access via INTERNET to both CONUS and OCONUS commercial, academic, private and foreign sources mandates both current and future course changes in order to maximize intelligence cost-effectiveness and open source availability to multiple echelon consumers.

Policymakers, military commanders, and force developers must track an ever increasing array of political, economic, social and military developments around the world where open sources provide significant contributions. The era of "information warfare" and "information dominance" requires mastery of open source collection, timely exploitation, development of a new "cyberspace" data base capability and improved electronic dissemination.

The Army considers Open Source Information (OSI) an essential input to all-source analysis and operations. Its vision for harnessing this critical resource for Force XXI is:

"To leverage OSI in the production of fused intelligence presentations responsive to the commander's requirements. Skilled soldiers, both Active and Reserve, and civilians supported by a wide range of tools will be the key element in acquiring, filtering and presenting this information.

Central to this vision is the understanding that OSI is expanding exponentially and is largely unrestricted. Furthermore, OSI is characterized by varying degrees of accuracy, levels of reliability, and cultural points of view. Leaders, soldiers, and civilians will need to possess high order analytical skills, the tools to process information and systems to allow collaborative efforts.

OSI will be fused with other sources of intelligence and may be integrated into the intelligence presentation at virtually any echelon and can be applied to varying degrees across the continuum of military operations."

The 21st Century Information Age will provide both opportunities and challenges in maintaining "information dominance" and executing "information warfare." U.S. strategy and military doctrine has changed from the "cold war prescriptive era" to one of "flexible response" to deal with the multipolar world and technological advances.

We also included in our vision the fact that a majority of 21st Century U.S. military operations will be concentrated in the Intelligence Community's Tier 3 and 4 countries, where General Military Intelligence (GMI) and Scientific and Technical Intelligence (S&TI) database holdings are deficient/insufficient and lacking in both quality and quantity.

The number and types of open source databases and networks have become exponential. This trend has already resulted in "information overload." Connectivity is rapidly expanding the availability and dissemination of information. Worldwide, a new network comes online every 20 minutes.

To meet this critical challenge, new analytic tools for 2010 will need to be developed in two categories -- **pre-analysis and exploitation:** Pre-analysis tools are needed to screen, find, capture, compile, extract, index, and prepare the data for analysis. Exploitation tools are needed to search, retrieve, and display the pre-analyzed data in advanced ways, using techniques such as visualization to aid in its understanding.

Information technology has increased in complexity and capability and has become indispensable to combat operations. Modern military forces are becoming totally dependent upon it to maintain, deploy and employ almost every weapon system in their arsenals. Technology has become a weapon in its own right, and information technology is being viewed as a "handmaiden of the instruments of war."

This premise also raises some questions about war and victory in the 21st Century - When does war begin? How should it be fought? How do you define victory? How will information-based warfare change doctrine, force structure and military strategy in 2010? Joint doctrine will need to include "nonlethal" Information Warfare (IW) and the role of open source information in its planning for robust C4I capabilities.

The use of open source information in IW will probably occur long before a shot is fired and that success in combat is likely to rely on IW campaigns. Furthermore, <u>information dominance</u> in some future scenarios may allow us to prevail without resorting to military force. Such scenarios would allow those combatants with superior IW capabilities to neutralize or deny weaker information dependent foes by altering interdicting, or destroying information and information assets, thereby <u>determining</u> the outcome of a crisis or actual military operations.

The future of 21st Century U.S. military and "coalition operations" requires that greater attention be paid to not only to the inter-operability of weapon systems but also U.S. and foreign information systems.

GOALS AND OBJECTIVES

The following Army open source goals and objectives have been established to achieve and maintain "Information Dominance" in 2010:

a. GOAL: **Determine which Army information requirements can best be met by OSI to satisfy commander's information needs.**

Objectives:

(1) Integrate open source into the intelligence requirements management system.

(2) Identify warfighter, policy maker, and user information needs that can be met by open source, tailored to the strategic, operational and tactical levels.

(3) Develop an evaluation and appraisal system to determine how well OSI has satisfied needs, to include validation of open source authenticity.

b. GOAL: **Establish an Army OSI Program Management Office.**

Objectives:

(1) Designate the commander USAINSCOM as the program manager for the Army open source program.

(2) Develop an Army information warfare open source doctrine.

(3) Expand the Peacetime Utilization of Reserve Component program to resource the RC MI OSIS for accessing, acquiring, processing, distributing and manipulating open source information. RC units should be considered from two perspectives when it comes to OSI exploitation: (1) as consumers of OSI in fulfilling a priority intelligence production mission; and (2) as designated collectors/processors of OSI for other intelligence producers.

c. GOAL: **Integrate the open source program within the Army Intelligence Investment Strategy (I^2S).**

Objectives:

(1) Establish and maintain a programmatic (PPBS) infrastructure and resource base of personnel, organizations, programs, and budgets for Army open source within the NFIP and TIARA programs.

(2) Invest in training, automated tools, database management systems, human resources and acquisition of

information sources and services to modernize open source capabilities.

(3) Perform cost-benefit analyses of program activities to maximize resource investments and perform value-added analyses which assists in tailoring the open source program to meet warfighter requirements.

(4) Provide RC MI capabilities which enable reservists to access, scan, browse, search, and retrieve from the expanding volume of OSI in multiple media and languages.

d. GOAL: **Provide communications and information distribution within the Army to enable exploitation of OSI in support of the full spectrum of contingencies.**

Objectives:

(1) Establish full connectivity and expand access to the IC OSI System (OSIS), to the Open Internet, and to commercial information providers.

(2) Integrate open source connectivity and analytical tools into the overall Army intelligence architecture at all levels, including analytical platforms (ASAS), communications systems (JDISS, InteLink, Trojan Spirit), topographic engineering analysis platforms (DTSS, ERDASS), and their successor systems.

(3) Integrate the reserve components into the open source system, to include Regional Training Sites (Intelligence), intelligence centers identified in the Peacetime Utilization of the Reserve Components, and selected individual ready reservists.

(4) Ensure the open source system is flexible, scalable, and compatible at all levels to support deployment of tailored intelligence support elements for full range of contingency operations, including support to task forces operating in an unclassified coalition environment.

(5) Ensure the Army open source capabilities are developed in conjunction with other service and joint service systems, to permit maximum joint interoperability.

(6) Develop a cadre of experts in OSI exploitation.

e. GOAL: **Provide Army Intelligence users at the strategic, operational and tactical levels with the capability to correlate, evaluate, analyze, synthesize, and interpret OSI to enhance situational awareness in response to their commanders' requirements in near real-time.**

Objectives:

(1) Develop and deploy the capability for Army users of open source to discover and retrieve information from unlimited sources through a single query interface.

(2) Develop and deploy the capability to prepare the acquired information for analysis, i.e., formatting, conversion, normalization, machine translation and automated processing.

(3) Develop and deploy the capability for Army users of open source to interpret, correlate and fuse OSI with other intelligence information, to include unlimited peer collaboration, and present the results visually to the commander in near real-time.

f. GOAL: **Apply proven commercial and government technology and best practices to all open source activities.**

Objectives:

(1) Monitor information technology developments and practices in the rest of the government and commercial world and test commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) solutions for meeting strategic, operational and tactical requirements.

(2) Invest NFIP, TIARA and JMIP funds in the integration of proven new enabling technologies critical to improving appropriate open source activities, rather than in R&D for the technologies.

(3) Leverage ongoing and planned Advanced Technology Demonstrations (ATDs)/Advanced Concepts Technology Demonstrations (ACTDs) and Advanced Warfighting Experiments (AWEs).

g. GOAL: **Provide capabilities for supporting Information Warfare through open source systems to ensure that the commander maintains Battlespace Information Dominance.**

Objective:

(1) Develop and deploy an OSI exploitation capability, which can respond to the immediate and long-range needs of C2 Protect and C2 Attack operations (e.g., Psychological Operations, Counterintelligence, civil-military operations, etc.) in the global information environment across the spectrum of conflict.

(2) Develop the capability to identify and exploit open source information and information systemsto support the commanders C2 Attack requirements.

(3) Develop the capability to identify and exploit instances of use of global and regional OSI systems by adversaries, to deceive, deny and disrupt friendly use of OSI.

h. GOAL: **Ensure a protected operating environment of Army users of OSI that provides for data integrity and continuity of operations.**

Objectives:

(1) Develop and maintain an Army information architecture that allows users from their work environment, whatever their respective security configurations are, to use OSI distributed throughout the Army, the IC and elsewhere.

(2) Protect Army held, networked, unclassified data holdings from inadvertent manipulation, deliberate intrusion or unauthorized use.

(3) Adopt procedures to safeguard against the flow of classified information into the unclassified environment.

(4) Develop and implement procedures to preclude the inadvertent disclosure of operational plans and intentions.

(5) Coordinate with COSPO to ensure protection of intellectual property rights.

OSS '95: THE CONFERENCE Proceedings, 1995 Volume II Fourth International Symposium on Global Security & Global Competitiveness: O - Link Page

Previous	Mr. Ed Dandar, Army Intelligence Open Source Program
Next	Maj. Mats Bjore, Swedish Military Open Source Program

Return to Electronic Index Page