

OPERATIONAL INFORMATION SHARING

*Working to Bring the Benefits of the Net-Centric Data
Strategy to the Warfighter*

March 2009



Distribution Statement A

Approved for public release: distribution is unlimited.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE

30 MAR 2009

2. REPORT TYPE

Study

3. DATES COVERED

01-09-2007 to 30-03-2009

4. TITLE AND SUBTITLE

Operational Information Sharing Working to Bring the Benefits of the Net-Centric Data Strategy to the Warfighter

5a. CONTRACT NUMBER

FA8771-04-D-0006

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Susan Cox; Ron Kelly; Tricia Spencer

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen Hamilton, 8283 Greensboro Drive, McLean, VA, 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

DoD CIO Enterprise Services & Integration Directorate, 1851 S Bell St, Arlington, VA, 22202

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Program Decision Memorandum III directed DoD CIO to report on implementation of the Net-Centric Data Strategy. One finding was to increase efforts to bring the advantages of information sharing to the warfighter. In response to this finding, the DoD CIO has identified early adopters and collaborated with these forward looking organizations across the extended defense community to understand the challenges and possible solutions for Operational Information Sharing - in simple terms, accomplishing the DoD mission by leveraging direct, day-to-day access to the vast network of information and expertise. This report describes efforts underway by the following organizations to improve information sharing at the warfighter level: Defense Technical Information Center Knowledge and Information Fusion Exchange Intelligence Community Enterprise Solutions USNORTHCOM Information Exchange Brokers As described in this report, a gap was found in operators' knowledge of the many information sources available to them. This gap is a result of many factors at play in the operator's environment including the number of information sources, the number of technologies and their rapid evolution, and the expertise needed to navigate the defense information network. To narrow this gap and improve Operational Information Sharing, the DOD CIO recommends 1. Explore the Combat Information Specialist role with USNORTHCOM and an additional COCOM. Defined by the Defense Science Board and demonstrated by USNORTHCOM's Information Exchange Brokers, the combat information specialists answer, research, and anticipate questions from commanders and operational users in the field. 2. Build connections between existing information providers and the warfighters. In the short term, DoD CIO can build connections among providers and operators via outreach and support of automated approaches. In the current state-of-the-Department as described in this report, Operational Information Sharing needs human intervention to ensure that the soldier/commander has all the relevant information to inform his decisions. Work continues in the government and private industry to refine policies and exploit the tools to automate search, access control, and retrieval. In the meantime, operational information sharing focuses on brokering information to augment the information advantage the warfighter has today.

15. SUBJECT TERMS

Operational Information Sharing, Knowledge Management, Combat Information Specialist, Information Exchange Broker

16. SECURITY CLASSIFICATION OF:

| | | | | | |
|----------------------------------|------------------------------------|-------------------------------------|-----------------------------|---------------------|---------------------------------|
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
| a. REPORT unclassified | b. ABSTRACT unclassified | c. THIS PAGE unclassified | Same as Report (SAR) | 35 | |

Executive Summary

Program Decision Memorandum III directed DoD CIO to report on implementation of the Net-Centric Data Strategy. One finding was to increase efforts to bring the advantages of information sharing to the warfighter. In response to this finding, the DoD CIO has identified early adopters and collaborated with these forward looking organizations across the extended defense community to understand the challenges and possible solutions for Operational Information Sharing – in simple terms, accomplishing the DoD mission by leveraging direct, day-to-day access to the vast network of information and expertise.

This report describes efforts underway by the following organizations to improve information sharing at the warfighter level:

| Organization | Information Sharing Mission Description | Example Success Story |
|--|--|--|
| Defense Technical Information Center | World-class array of scientific and technical information to support defense | Brokered information on chemical agents for USNORTHCOM |
| Knowledge and Information Fusion Exchange | Watch center support for IED Defeat and Irregular Warfare information | Provided IED Initiator usage information for the Iraq Multi-National District-Center in a day |
| Intelligence Community Enterprise Solutions | Platform and tools for mass collaboration and information sharing | Allowed a COCOM user to receive timely, authoritative feedback about indirect fire attacks on a base in Iraq |
| USNORTHCOM Information Exchange Brokers | Proactive monitoring of information across mission partners | Aided coordination of fire-fighting assets during California wildfires |

As described in this report, a gap was found in operators’ knowledge of the many information sources available to them. This gap is a result of many factors at play in the operator’s environment including the number of information sources, the number of technologies and their rapid evolution, and the expertise needed to navigate the defense information network. To narrow this gap and improve Operational Information Sharing, the DOD CIO recommends:

1. **Explore the Combat Information Specialist role with USNORTHCOM and an additional COCOM.** Defined by the Defense Science Board and demonstrated by USNORTHCOM’s Information Exchange Brokers, the combat information specialists answer, research, and anticipate questions from commanders and operational users in the field.
2. **Build connections between existing information providers and the warfighters.** In the short term, DoD CIO can build connections among providers and operators via outreach and support of automated approaches.

In the current state-of-the-Department as described in this report, Operational Information Sharing needs human intervention to ensure that the soldier/commander has all the relevant information to inform his decisions. Work continues in the government and private industry to refine policies and exploit the tools to automate search, access control, and retrieval. In the meantime, operational information sharing focuses on brokering information to augment the information advantage the warfighter has today.

Contents

| | |
|--|-----|
| Executive Summary | i |
| Contents | ii |
| Figures | iii |
| Introduction..... | 1 |
| The Power of Information Sharing | 2 |
| Operational Information Sharing Can Benefit the Operator..... | 4 |
| A DSB Approach to Operational Information Sharing..... | 6 |
| Existing Efforts Support Information Sharing..... | 9 |
| Intelligence Community Enterprise Solutions..... | 9 |
| Defense Technical Information Center | 10 |
| Knowledge and Information Fusion Exchange..... | 12 |
| USNORTHCOM Information Exchange Brokers..... | 13 |
| Findings..... | 14 |
| Recommendations to Improve Operational Information Sharing | 17 |
| Appendix A, References | 20 |
| Appendix B, Results from Partner Efforts..... | 21 |
| Defense Technical Information Center | 21 |
| Knowledge and Information Fusion Exchange..... | 25 |
| Intelligence Community Enterprise Solutions..... | 28 |

Figures

| | |
|--|----|
| Figure 1, Information Sharing Facilitates the Evolution of a Device for IED Defeat..... | 3 |
| Figure 2, Operational Information Sharing | 5 |
| Figure 3, Approach for Operational Information Sharing | 7 |
| Figure 4, ICES Provides an Enabling Platform for All Roles | 10 |
| Figure 5, DTIC and IACs Provide Knowledge Management and In-Depth Expertise..... | 11 |
| Figure 6, KnIFE Focuses on Irregular Warfare Topics | 13 |
| Figure 7, IEBs Provide the Combat Information Specialist Role to USNORTHCOM | 14 |
| Figure 8, Existing Efforts Provide Operational Information Sharing Capabilities..... | 15 |
| | |
| Figure A- 1, Number of Pages and Hits for September 2008 | 27 |
| Figure A- 2, Number of Unique Servers, Visits, and Downloaded Bandwidth, Sept 2008 | 27 |
| Figure A- 3, Number of Hits from Sept to Dec 2008..... | 27 |

Introduction

In 2003, the Office of the Department of Defense (DoD) CIO completed the *Net-Centric Data Strategy (NCDS)* for the Department of Defense which led to a DoD directive on data strategy¹ as well as a companion implementation guide². A few years later the same office developed a strategy for net-centric services that highlighted the evolution of DoD's information technology approach to enterprise services. All of these documents taken together formed an innovative conceptual framework for transforming the way DoD approached the sharing of information. Until these new documents were postulated, the focus was on point-to-point sharing of information; if a sender of information knew his intended recipients, the sender transmitted information to those known receivers and only those. There was no inherent motivation to share information with other users, much less with an unanticipated, but authorized user.

These new strategies changed the mindset of information sharing inside DoD and began to target these unanticipated, but authorized users. Thus information sharing and enterprise services began to evolve. But there was a looming problem to this information sharing revolution — just because an innovative strategy was published and understood by the technically proficient in the Pentagon did not mean the wider audience understood, much less was even aware of the new strategies. In addition, there was a need to determine if military forces in the field — the warfighters — were aware of these new concepts and how the new strategies could be applied to operational matters.

During the DoD budget review cycle in 2006, the Deputy Secretary published a Program Decision Memorandum (PDM) that directed the DoD CIO to assess the progress and understanding of these new net centric strategies and report the findings. A subsequent 2006 DoD CIO report³ found that the **value of the *Net-Centric Data Strategy* remains largely unrealized by the Department's business, warfighting and intelligence operators.**

That finding was the basis for the CIO's Information Policy and Integration (IP&I) Directorate work in Operational Information Sharing (OIS). In 2006, the IP&I office began a task in collaboration with Defense Information Systems Agency (DISA) to address the challenges to information sharing. The initial focus of the task was to examine how information sharing services might be monitored and managed. Through support to the NetOps Community of Interest and DISA, a concept of operations was developed, and a pilot of enterprise service monitoring of information sharing services was designed and demonstrated. In the second year, the IP&I focus shifted from the network-oriented back-end to the consumer— specifically how

¹ Department of Defense Directive 8320.02: "Data Sharing in a Net-Centric Department of Defense"

² *Guidance for Implementing Net-Centric Data Sharing*, DoD 8320.02-G

³ *Department of Defense Implementing the Net-Centric Data Strategy Progress and Compliance Report*, September 14, 2006

operators may access and use information sharing in accomplishing their missions. The Directorate's OIS Study team examined ways that information sharing might benefit the warfighter and as a result, identified DoD agencies that were already addressing portions of the information sharing activities.

To build on the OIS Study team's understanding of operational information sharing, the team selected a trio of DoD component agencies as partners and worked with those partners to explore information sharing from several unique angles. The Intelligence Community Enterprise Solutions (ICES) group had already achieved much success and recognition in the information sharing realm so they were chosen to ensure we did not "re-invent the wheel." The OIS Team saw an opportunity with them to gain insight into the use of information sharing tools. A second organization, the Defense Technical Information Center (DTIC) had been a long-time leader in the defense technical information world and was seeking to bring its expertise to the warfighter by assisting COCOMs with information sharing during exercises and operations. It appeared to match the intent for year number two. The third office, the Knowledge and Information Fusion Exchange (KnIFE) had been presented with a short term challenge to stand up a web portal to share near real-time information DoD-wide on the Improvised Explosive Device (IED) threat; their work also fit the mold of what the OIS Team was trying to analyze. As a result, the OIS team chose these three organizations with which they could share some dedicated PDM funding so the organizations could expand their capabilities in the area of information sharing as it pertains to operations.

The intent of this report is to present the results of the past year investigating Operational Information Sharing and working with the partner organizations. First, several illustrative examples selected by the OIS team are discussed to show how timely sharing of information can lead to successful operations. This report then describes how a recent Defense Science Board (DSB) summer study addressed a similar information sharing problem within DoD. The DSB recommended that the addition of a unique information specialist may be needed to transition the enterprise from point-to-point communications to many-to-many communications enabling the unanticipated user to benefit. This report will examine in more detail just how each of our selected organizations works to support warfighters' missions through information sharing. Finally, findings from this year of investigation and several recommendations for follow-on actions are presented.

The Power of Information Sharing

To many operators, information sharing seems like a term used by computer technologists; it does not appear to have a direct association to their day-to-day tasks. In today's world, information sharing has the power to influence the success of national security. The DoD identifies information as a strategic asset⁴. To make use of this strategic asset, we must have means of sharing the information across the defense enterprise. Consider this improvised

⁴ Department of Defense Information Management & Information Technology Strategic Plan 2008-2009

explosive device (IED) example of what is possible with information sharing among military operators:

"By late summer 2005, the explosively formed penetrator (EFP), like the underbelly IED, had become an appallingly lethal weapon for which there was no obvious countermeasure."⁵ Several approaches were attempted by the IED Task Force, with mixed results, "meanwhile, soldiers in the field pursued their own solutions".⁶ Because a passive infrared sensor reacted to heat signatures, one inventive trooper proposed mounting a giant hair dryer on a bumper to blow hot air in front of the vehicle. Another took a toaster purchased at a bazaar, plugged it into his Humvee and dangled the glowing appliance from a long pole welded to the front of the vehicle. The soldiers shared their ideas on the companycommander.net web site in hopes of building on each other's experiences to identify a better solution.



Figure 1, Information Sharing Facilitates the Evolution of a Device for IED Defeat

A similar but more practical idea, also proposed by a soldier, became a countermeasure called Rhino - a glow plug -- a pencil-shaped object with an electrical heating element, often used in diesel engines -- was placed inside a metal ammunition can, which was then attached to a metal pole 10 feet in front of a Humvee or truck. The red-hot can decoyed the infrared sensor into triggering prematurely so that the copper EFP, an armor-piercing explosive slug fired at the Rhino rather than the vehicle. This solution was also shared on companycommander.net, getting the information across battalions quickly. By sharing the solution directly among soldiers in the field, the Rhino concept was put to use even as the IED Task Force worked to fund, test, and develop the production version for roll-out across the force.

⁵ http://www.washingtonpost.com/wp-dyn/content/article/2007/10/01/AR2007100101760_pf.html

⁶ Ibid.

In the examples above, the soldiers in the field, the operators, had direct access to experiences and ideas of their peers. The information they were able to share provided a positive impact on the success of their missions. This ability to share and access mission-relevant information is what we are referring to as Operational Information Sharing.

Another example of Operational Information Sharing:

During Hurricane Katrina, the response teams were faced with an unexpected problem: many residents of New Orleans and surroundings were forced to leave their pets behind during the hurried evacuation. As is sometimes the case, several organizations were doing their best to help with the problem, but were not aware of the other's efforts. The 82nd Airborne and other military units were rounding up pets and trying to purchase cages for them. At the same time, the SPCA had available cages but did not have the ability to round up the pets. As part of their hurricane response effort, USNORTHCOM had deployed a person to the Joint Task Force headquarters to focus on sharing information across the many mission partners responding to the hurricane. This person, an information broker, is trained to identify gaps and seams in information sharing. Due to their focus on information sharing across disparate groups, the information broker was able to help bring together the SPCA and the appropriate military units to deliver the animals to the locations where cages were already available.⁷

This effort demonstrates how information sharing matched the need with the available equipment in an efficient manner. In this case, the information sharing was facilitated by human intervention — the information broker. With the ad hoc nature of mission partnering in the high tempo environment of response to Katrina, a diverse set of organizations was involved in the response: the military, civilian agencies, state government, non-governmental organizations, and local responders. Because of the myriad of helping partners, the information broker was a key ingredient in accomplishing the mission by tying together the need with the supply. In this case, the information broker was the unanticipated user of information from the SPCA and the 82nd Airborne unit.

Operational Information Sharing Can Benefit the Operator

These examples demonstrate the potential value of Operational Information Sharing – that is, accomplishing a mission as a result of direct, day-to-day access to the vast network of information and expertise focused on the nation's defense. As shown in Figure 2, in an Operational Information Sharing environment, operators have access to communication

⁷ Discussions with USNORTHCOM Information Exchange Broker

users to access data without any delay for processing, exploiting, or disseminating. In the case of the stranded pets during Hurricane Katrina, the information broker's ability to tap into the information from different organizations in a timely manner resolved a problem efficiently. If those organizations had communicated in a point-to-point manner and waited for each partner to publish current status, they may have missed their opportunity.

While these success stories show the promise of the department's information sharing vision to "deliver the power of information to ensure mission success..." as set forth in the *Information Sharing Strategy*, the problem is that today's information sharing environment is not well understood. Unlike the situation during Hurricane Katrina, there is no cadre of DoD information brokers to ensure the information gets to both user and provider. Unlike the development of the Rhino on companycommander.net, it is not clear to most operators where and when to post their questions on a network in order to get the best response; it is not clear where and when to post their experiences to make it available to others who might benefit. These are the kinds of connections and connectors of information the OIS Study team was trying to find.

A DSB Approach to Operational Information Sharing

At the same time that the PDM data strategy progress report recommendations were being acted upon in 2006, the Defense Science Board (DSB) was working on the related question of assessing DoD's progress toward achieving a robust and adaptive net-centric information management system. The results of the DSB work, as documented in the report published in 2007 titled *Defense Science Board 2006 Summer Study: Information Management for Net-Centric Operations Vol. I and Vol. II*, provide an approach for giving operators the relevant, day-to-day information sharing the team believes can benefit their missions.

Within the report, the DSB notes that "combat information management involves the seamless, timely flow of information between and among a globally connected set of partners. The task force concludes, however, that commanders and tactical level combatants will need assistance in managing critical information needs until better information management tools can be created in the future"⁸.

Three Roles Are Needed to Support the Operators

The DSB report notes that limited efforts have been made to make sure needed information is available to the warfighter. In contrast, commercial enterprises invest in knowing and extracting relevant information for its larger staff, particularly in industries that rely on information as their competitive advantage. For example, Accenture is in the management consulting and technology services industry in which its information base and experience are its most valued corporate assets. Accenture recognized the importance of the information advantage and

⁸ *Defense Science Board 2006 Summer Study: Information Management for Net-Centric Operations Vol. I, page 18*

assigned more than 150 “information managers” whose job it is to watch key industries and innovation areas and maintain a knowledge base of this information for the rest of the staff.

The information managers know the most relevant information sources, best practices, and key subject matter experts in their focus areas. They are responsible for the quality of the information they manage and making that information available to those who need it throughout the company.

The differentiator to this approach is that the focus is on the information, its quality, and its currency, rather than on the technology infrastructure used to store and publish it. To address this gap, the DSB recommends new skill sets be created called “combat information specialists” augmented by knowledge managers and subject matter experts. Together these three roles — using the defense enterprise network of infrastructure and tools — provide an approach for Operational Information Sharing as shown in Figure 3.

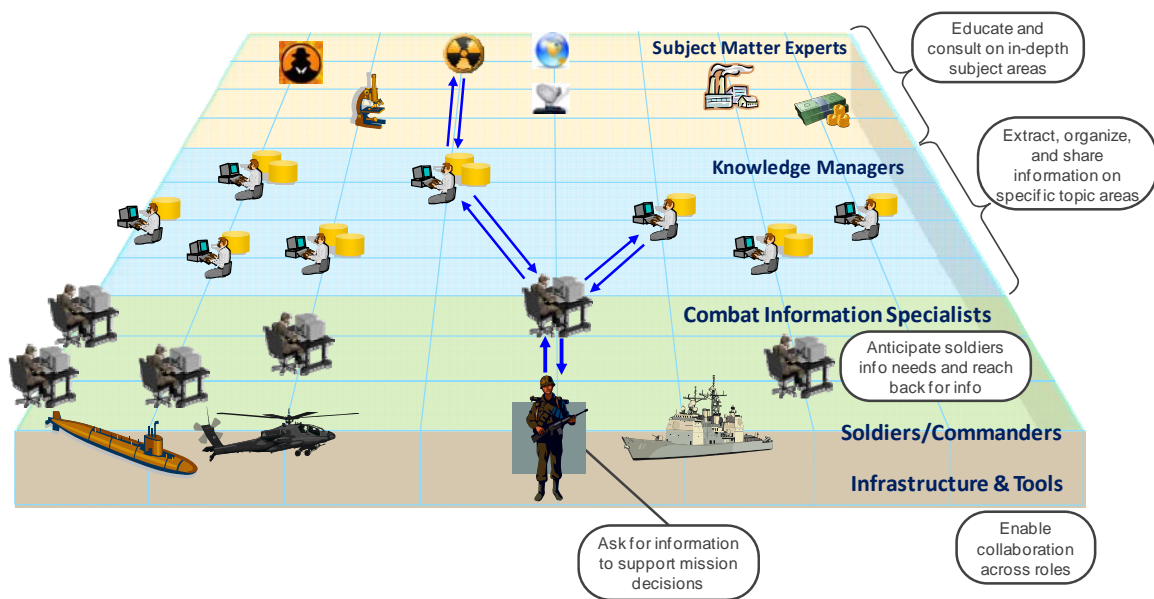


Figure 3, Approach for Operational Information Sharing⁹

As articulated by the DSB, “the creation of three distinct levels is recommended. At the first level, closest to the operator in space and time, combat information specialists answer, research, and anticipate questions from commanders and operational users in the field. In developing answers to those questions, they may collaborate with combat information specialists supporting other units and commanders and/or they may work with knowledge managers whom identify, discover, extract, organize, catalog, and maintain information about a selected set of topics. Knowledge managers, and others, use subject matter experts, who

⁹ Adapted from the *Defense Science Board 2006 Summer Study: Information Management for Net-Centric Operations Vol. I*, page 19.

provide in-depth knowledge, advice, and consultation in highly specialized areas.”¹⁰ In meeting operational needs, the combat information specialist is envisioned as an essential element of the unit fighting team requesting and disseminating critical information to combatants, both in mission preparation and in real-time support of mission execution. For further discussion of the roles, please refer to the DSB report.

Three Roles Provide the Scale Needed for the Defense Community

As described, the approach for Operational Information Sharing allows for human intervention to ensure that the soldier/commander has relevant information to inform his decisions. Work continues in the government and private industry to develop approaches and tools to automate search, access control, and retrieval. In the meantime, this operational information sharing approach can take advantage of the information advantage available from information providers today.

The scale of the Department provides a challenge in meeting our goal to give operators day-to-day, direct access to all those in the extended community supporting its mission. The separation and clarification of the roles of knowledge manager and combat information specialist provide a key to scaling information management to the size of the national defense mission. An operator’s mission is likely to span multiple subject areas, and without a combat information specialist involved, the role of bringing the information together might fall upon a knowledge manager. While the knowledge manager has a desire to help, he likely does not have expertise or the awareness of other sources of information available. The job of the combat information specialist is to know about available information sources and enterprise services, and to synthesize information accessed for the immediate context. From the knowledge manager’s perspective, the combat information specialist role provides a focal point for outreach and alleviates the need for the knowledge manager to advertise capabilities to the general warfighter community.

If the knowledge manager is removed from the framework, the combat information specialist is left with the daunting task of determining who the experts are in each field and vetting all information sources for themselves. These tasks are most efficiently accomplished with someone who can focus on a particular subject area – the knowledge manager. For example, consider the subject area of piracy which plagues both Asia and Africa. To best support efforts of both CENTCOM and AFRICOM, a knowledge manager focused on piracy information and expertise could be available to combat information specialists at both COCOMs to aid in their discovery and use of piracy information.

By allowing personnel to focus on their skill set and/or their subject area of expertise, they are better positioned to make the connections needed across the extended defense community, and to match the information from multiple sources with the mission.

¹⁰ *Defense Science Board 2006 Summer Study: Information Management for Net-Centric Operations Vol. I, page 20*

Existing Efforts Support Information Sharing

Is the vision put forth by the DSB too grandiose? It turns out, that within the extended defense community, organizations and efforts have been grappling with pieces of the vision – and found both successes and challenges.

Throughout 2008, the OIS Study team identified and collaborated with several groups in the extended defense community to explore and better understand how to support the operator with information sharing efforts already underway. In this section, four specific organizations are introduced. In each case, the discussion includes the organization’s mission relating to information sharing and how that mission fits into the approach for Operational Information Sharing as shown in Figure 3. Lastly, if that organization partnered with the DoD CIO specifically for Operational Information Sharing, a description of that collaboration is included.

Intelligence Community Enterprise Solutions

Intelligence Community Enterprise Solutions (ICES) is an organization within the Director of National Intelligence (DNI) CIO that has been enabling information sharing for over a decade. ICES provides a platform and set of tools, collectively referred to as Intelink¹¹, that intelligence analysts throughout the Intelligence Community (IC) and the DoD use to connect with colleagues, search for intelligence information, and post their own findings. Of particular note, the search tool provided by ICES is used on Intelink and by other organizations’ portals as well. This search is being adapted to be the joint DoD and DNI enterprise search service. Another tool provided by ICES is Intellipedia which uses wiki technology for mass collaboration on intelligence and related information. Intellipedia has over 700,000 pages of articles across three security enclaves, ranging from a coordination portal for a hurricane to articles discussing terrorist attacks in Pakistan.



As shown in Figure 4, ICES provides tools and infrastructure that make it possible to communicate and share information. While originally focused on the intelligence analyst user group, Intelink has a large base of users throughout the extended defense community. Other organizations are modeling their efforts to build on the success of Intellipedia by developing similar wikis for their communities including the Department

Authoritative Feedback via Intelink

A COCOM user posted an article from the Air Force Intelligence Agency (AFIAA) on their group’s Intelink Blog. The article’s topic was indirect fire attacks on a base in Iraq. The analyst in Iraq whose numbers and research had been quoted in the article saw the Blog item. Through the Blog platform, the analyst noted that things were a bit different than how they had been interpreted by the AFIAA. The Blog was immediately updated with the authoritative information. The benefit to the COCOM users: they never would have received that critical feedback through the old communication mode, a readfile, which only went to a limited audience through an email distribution list and never received comments/feedback from other intel analysts, especially in a time-critical situation.

¹¹ <https://www.intelink.gov/>

of State’s Diplopedia covering foreign affairs and DoD Techipedia recently launched by DTIC. The challenge across these wikis is to ensure that users are able to discover information from any source that is relevant to their mission.

The OIS Study team worked with ICES to explore how defense operators were using the Intelink tools and infrastructure. A survey of a subset of COCOMs found that the search tool is the most widely used tool and is considered the most valuable by the operators. For more information on the OIS team’s collaboration with ICES, please see page 28 of Appendix B, Results from Partner Efforts.



Figure 4, ICES Provides an Enabling Platform for All Roles

Defense Technical Information Center

The Defense Technical Information Center¹² was established just after World War II as the Air Documents Research Center (ADRC) and evolved



to become a DoD Field Activity charged with maintaining a world-class collection of scientific and technical information to support the defense mission. DTIC fulfills the role of Knowledge Manager for the science and technology subject areas as shown in Figure 5. DTIC is constantly updating and adding to its information collection through its relationships within the defense community, academia, and private industry. DTIC is able to make information from across these communities of subject matter experts available to the extended enterprise through its portal.

¹² <http://www.dtic.mil/dtic/>

Another service operated by DTIC is the Information Analysis Center (IAC) program. IACs¹³ are research and analysis organizations established by the DoD to support researchers, scientists, engineers, and program managers with expertise in all areas of Defense research and engineering including Materials, Manufacturing, and Testing; Chemical, Biological, Radiological, and Nuclear Defense; Reliability; and Weapons Systems Technology. By focusing on a specific topic, an IAC can provide cutting edge information and reach back to experts in the field. As shown in Figure 5, IACs primarily provide the role of Subject Matter Experts with a secondary role in knowledge management of the information.



Figure 5, DTIC and IACs Provide Knowledge Management and In-Depth Expertise

DTIC recently demonstrated its potential value to the operator by participating in exercises with PACOM and NORTHCOM. During these exercises, on-site personnel from DTIC were able to reach back into the scientific collections and IACs, and pull together and synthesize information for the missions.

Feedback from the exercises confirmed the value of the information available from DTIC to the missions. DTIC's challenge has been to raise awareness of its services to those in the field. Over the last half of Fiscal Year 08, the DoD CIO OIS project has supported DTIC in

¹³ <http://iac.dtic.mil/>

Brokering Information on Chemical Agents

As a participant in USNORTHCOM's Ardent SENTRY 2008 exercise, the DTIC reference librarian provided research in response to several scenario-driven events. For example, an incident occurred at one of the chemical depots. In response the embedded librarian with reach back to the IACs acquired information on the release of chemical agents from DTIC's Science & Technology Network, IAC databases, and third-party sources. This information was analyzed and consolidated into a searchable document made available on the USNORTHCOM Interagency Coordination Group's shared drive, providing quick/easy access for the command group decision makers. The Chief Concepts & Technology Division USNORTHCOM stated, "I hope our collaboration can continue as DTIC capabilities have great potential to increase the Command's effectiveness during homeland defense and civil support operations and exercises."

raising their profile with the Combatant Commands (COCOMs). By delivering operational information sharing, more soldiers, sailors, airmen, and marines in the field will benefit from this deep expertise by facilitating the connections back to DTIC and the appropriate IACs. For more details of DTIC's efforts in Operational Information Sharing see page 21 of Appendix B, Results from Partner Efforts.

Knowledge and Information Fusion Exchange

In response to the changing battlefield encountered during Operation Iraqi Freedom, Knowledge and Information Fusion Exchange (KnIFE)¹⁴ was established in 2006 to provide warfighters with current information on IED defeat methods, technology, and best practices. In six months, KnIFE, based within US Joint Forces Command, was able to field the capability by providing a focused web site that provides visibility of and access to IED defeat information. On the web site, an operator can discover and access information. Further, an operator can fill out a Request for Information which is answered by personnel in the KnIFE watch center.



KnIFE fulfills the Knowledge Manager role for IED defeat subject matter by vetting information, organizing information, and developing the network of experts for in-depth knowledge when needed. For those operators who are aware of and contact KnIFE, KnIFE also provides some level of the Combat Information Specialist role by understanding the battlefield environment and answering mission-specific requests from the operator. This is shown on Figure 6.

The DoD CIO worked with KnIFE to enable the expansion of their information capability to cover the broader topic area of Irregular Warfare. As a result, a second KnIFE site focused on Sniper Attacks is now available to the warfighters. KnIFE is monitoring its use in order to continue evolving the capability. See page 25 of Appendix B, Results from Partner Efforts for more information on this effort.

IED Initiator Information Provided in a Day

KnIFE's 24/7 Request for Information (RFI) Watch Cell responds to Improvised Explosive Device (IED) and other Irregular Warfare (IW) questions from warfighters and interagency personnel worldwide. Recently KnIFE received an RFI from a military planner in Iraq. In order to facilitate detailed planning for jamming support of operational units, he wanted to know the most common Radio-Controlled IED initiators used by insurgents in one of the coalition regions in Iraq. KnIFE responders were able to provide an answer in less than three hours which included monthly, bi-monthly, and quarterly summaries of known IED initiators in the specified region. The RFI was closed by the requestor at the end of the day. KnIFE's rapid and complete response to this request furthered the mission of our warfighters downrange by providing a single point for IW information requests.

¹⁴ <https://knife.jfcom.mil/>

As with DTIC, KnIFE continues to grapple with how to reach those who will benefit from its capability. KnIFE produced a video describing its services to be played for deployed warfighters through the Armed Forces Network. Through their home organization, Joint Forces Command, they have inserted materials in pre-deployment training to inform potential consumers.



Figure 6, KnIFE Focuses on Irregular Warfare Topics

USNORTHCOM Information Exchange Brokers

With the standup of USNORTHCOM in 2003-2004, the leadership of the J6 wanted to ensure support for information sharing and capabilities by establishing the Information Synchronization Group (ISG). As part of the ISG, experts were embedded through the staff to help with synchronization of information; over time, these personnel were called Information Exchange Brokers (IEB). While the ISG focus has changed over time, the IEB concept has continued to grow and mature at USNORTHCOM.

USNORTHCOM IEBs are personnel who proactively monitor mission-relevant information in order to be ready for any events in their area of responsibility. The IEBs facilitate cross-organizational information sharing that is particularly critical for this command to support civilian authorities. The cross-organizational information sharing must occur among the command's operational cells and the many mission partners from



IEBs Aid Coordination of Firefighting Assets

During the wildfires in southern California, IEBs at the USNORTHCOM headquarters were relaying to IEBs on the ground, the status of capabilities being brought into the Joint Operations Area. The IEBs on the ground assisted the commanding officer in coordinating best use of assets and posting deployment plans to the web. Then, the IEBs worked together to disseminate the website links to the appropriate first responders and command centers throughout the state. Success depended on getting the right assets to the right locations and then sharing information with the right agencies and users. California State Fire Marshal: "credited USNORTHCOM with being enablers of information by providing the fire operations incident commanders with real time operations information on a large scale that helped commanders in their decision making processes".

the federal civilian, law enforcement, intelligence and state and local communities. Practically speaking, the IEBs must be able to navigate the information environments and technologies being used across mission partners. They must also be able to translate the lexicons and jargon of these partners.

The USNORTHCOM IEB role appears very similar to the Combat Information Specialist role as shown in Figure 7. An IEB is working within a particular operational cell and is able to anticipate the needs of the cell’s mission. In addition, the IEB is monitoring partners’ information network and is working with IEB personnel in other cells in order to bring relevant information to the task. In the USNORTHCOM IEB model, the personnel are also knowledge managers for specific subjects.



Figure 7, IEBs Provide the Combat Information Specialist Role to USNORTHCOM

Findings

During the past year, the OIS Study team obtained a wealth of insight on how well the data and services strategies were being used at the operator level. We were heartened by the fact that much good work is taking place to assist the warfighter with the sharing of information. From new technologies in portals, to the use of an information exchange broker at various levels, it is evident that DoD is attempting to address the challenges of moving to solutions that enable information sharing across the extended enterprise of the DoD mission.

Finding 1: Significant information sharing to support the operator is already underway across the Department

Based on the DoD CIO work from Fiscal Year 2008, we found efforts underway across the Department to support the operators with information and to make that available through a variety of information sharing approaches. Figure 8 shows the aggregation of these efforts superimposed on the approach presented in this report.



Figure 8, Existing Efforts Provide Operational Information Sharing Capabilities

We found organizations — DTIC, IACs, and KnIFE — that are experts in specific subject areas and are managing the knowledge to make it useful to the operator and the rest of the defense community. ICES provides a platform and a set of tools to enable information sharing. We also found one organization, USNORTHCOM, that, while not their initial intent, tested the role of Combat Information Specialist and found it to be successful within their COCOM. Note that the efforts discussed here are only representative of those in the extended defense community that are working on improving operational information sharing. There are others including Defense Knowledge Online (DKO) —the enterprise portal for DoD —a platform for sharing among teams and with the larger community. It is DoD’s challenge to find ways to leverage these existing efforts into more robust information sharing for the entire defense enterprise.

Finding 2: There is an evolving set of information providers and venues for information sharing

Throughout the year, the OIS Study Team found many organizations providing information of value, but not all warfighters are aware of what is available to use. There is a compelling need for a diverse blend of numerous organizations to provide information that is unique and of value to the operators’ missions.

Some information providers were quickly established in response to a specific need to share information. For example, KnIFE was conceived and deployed quickly to address an urgent information gap in IED Defeat methods and technologies. As a result, the KnIFE founders chose the information sharing approach, technologies, and tools that best matched their stated mission and were able to deliver their solution quickly by focusing on their prime customer — the warfighter.

But does a targeted provider allow for unanticipated use of its information sources? Other organizations we worked with reached a broader audience to share valued information. For example, ICES provided Intellipedia originally as a tool for sharing information across the

extended intelligence community, but then broadened its reach to the larger DoD and IC enterprise. Rather than use the Intellipedia solely for the intelligence analysts to share information, this sharing service now can be used by all and has a greater chance to reach that unanticipated user. In order to truly support unanticipated use, a search mechanism is needed that can work across relevant information sources.

As we know, user needs and technologies change over time. For example, the ICES-developed Intelink Forums were in high demand for years and allowed free exchange of information and ideas. When ICES provided Intelink Blogs to its customers, the community moved quickly to use Blogs as a principal venue for sharing information. The resultant use of the Forums plummeted and recently the Forum application was discontinued. Anticipating the change in user needs and appropriate technologies enables the enterprise to be ready to exploit that change.

While it may seem simpler to have one provider of DoD information to the enterprise, it is not feasible, nor prudent, at this stage of the evolution of information sharing. In fact such a consolidation may be detrimental and not even feasible across such a large scale extended enterprise as DoD. Therefore, to achieve effective information sharing for the warfighter, we must assume there will continue to be many information providers, many venues for sharing, and constant change in technologies.

Finding 3: Commanders are not always aware of the available information

Given the scale of the DoD enterprise and the variations in its information environment, there is a great need for expertise about what information is available, how to discover that information, and how to most quickly access it. Currently, it is unrealistic to assume that all commanders can navigate the information environment in any depth without skilled assistance. As recently as 2007, the Defense Science Board concluded that “commanders and tactical level combatants will need assistance in managing critical information needs until better information management tools can be created in the future”¹⁵. The OIS Study team heard from one logistics specialist who found that it is sometimes challenging to know where to ask a question that falls outside the bounds of day-to-day tasks. This is consistent with the DSB’s conclusion.

Throughout discussions in the last year, we found that providers are working to raise awareness of their offerings but with limited success. Last winter, DTIC hosted a COCOM conference to raise awareness of their technical and information services. Surprisingly they found that several COCOMs had no prior knowledge of DTIC’s services or capabilities. Therefore, DTIC began to work more directly with a number of COCOMs to market and socialize their offerings. While progress is being made with a select number of the COCOMs, DTIC continues to address this real challenge of building awareness throughout the DoD community of users, specifically those in the field.

¹⁵ *Defense Science Board 2006 Summer Study: Information Management for Net-Centric Operations Vol. I, page 18*

Other organizations including the Center for Army Lessons Learned (CALL) and KnIFE also struggle with how to make their capabilities known to the practitioners who can most benefit from them. Approaches used by KnIFE are: (1) engaging with critical warfighter units preparing to deploy, (2) distributing printed materials describing KnIFE's capabilities at all pre-deployment training locations, (3) mass emailing updates to operations and intelligence staffs, and (4) distributing a short video describing KnIFE's capabilities on Armed Forces Network, which airs routinely to the warfighter in theater.

Each of the DoD organizations we investigated continue to creatively address the challenge of building awareness; but currently, they each take an ad hoc approach hoping to reach as many potential consumers as possible .

Finding 4: Documenting warfighting experiences and related information remains a challenge

The information providers we engaged consistently found that documenting warfighter experiences and information from the field poses a considerable challenge. While all DoD members know that documenting or posting official records is essential to the evolution of DoD best practices, keeping such records is often a low priority task for the warfighter. CALL found that their best successes in gathering valid inputs for lessons learned are achieved when they physically go to the field and interview the warfighters to capture their experiences.

NOTE: this report does not address the challenges to information sharing created by multiple networks, multiple security enclaves, and multiple information markings used in the DoD enterprise. Efforts are currently underway to resolve these complex issues including the DoD's Attribute-Based Access Control (ABAC) efforts and the federal government's Controlled Unclassified Information efforts. Consequently, the recommendations in this report focus on improving the operator's knowledge of information sources available to them and ability to apply information to accomplishing their operational missions.

Recommendations to Improve Operational Information Sharing

After a year's worth of investigation and discussion with only a few key DoD information providers, the OIS Study team barely scratched the surface of this ever expanding information enterprise that will grow more sophisticated in the coming years. The team offers the following recommendations for future endeavor:

Recommendation 1: Analyze in more depth the role of the Combat Information Specialist within USNORTHCOM and explore how other COCOMs might benefit.

To build on the success of the IEB effort within USNORTHCOM, the Operational Information Sharing effort for FY09 proposes to work with USNORTHCOM to better understand their IEB model and to identify an additional COCOM for piloting the IEB capability.

The USNORTHCOM IEB capability provides the role of Combat Information Specialist to the Command. The IEBs are assigned to operational cells within USNORTHCOM and are experts in sharing information across the information environments of their mission partners. As envisioned for the Combat Information Specialist role, IEBs understand their cell's mission and are able to anticipate information needs and to respond to requests posed by their commanders. As is the case with USNORTHCOM and their many non-DoD mission partners, there are other COCOMS who face similar information sharing challenges with multi-national, coalition, and non-governmental organizations. The role of Combat Information Specialist may be able to facilitate information sharing across these non-DoD entities by providing human intervention to broker and bridge across information sensitivity and network issues.

Pursuing this recommendation will further assess the Combat Information Specialist role by working with an additional COCOM and by training the specialists to understand the breadth of the knowledge managers and information infrastructure available to them beyond their COCOM. This effort will include work with the USNORTHCOM IEBs, across other COCOMs, and with the respective partner agencies.

Recommendation 2: Build connections between existing information providers and the warfighters

As noted in the findings, information providers continue to be challenged to ensure the rest of the community is aware of their capabilities. To help address this in the short term, the DoD enterprise needs to:

- 2.1 Build human-to-human connections among information providers and consumers. To increase awareness among organizations in the enterprise, the OIS Study team will post and publicize information sources in key sharing environments throughout the community. These postings will increase the likelihood that humans searching for relevant information sources will find sources of interest and make contact with those sources directly. This effort could include adding information to DKO and to Intelink and other collaborative or sharing environments. While posting to multiple sites may seem redundant, in the current state of the network, this may be necessary to effectively spread the word across the enterprise.
- 2.2 Enable a more automated approach where information providers ensure their offerings can be found through DoD's Enterprise Search. To meet the goals of information sharing, information providers need to make sure their information can be discovered by unanticipated, but authorized users. There are multiple strategies for achieving this based on the sensitivity of the information. In some cases, information sources can be indexed so that the Enterprise Search can be used to discover the information easily. In other cases, the information may have to be described in a catalog due to security restrictions. Either way, it is critical that the information be made visible to the enterprise so that unanticipated, but authorized users may discover it.

As the DoD CIO pursues ways to bring together information providers and operators to benefit the mission, it is anticipated that additional DoD organizations and toolsets providing valuable information and expertise will be uncovered. Improved operational information sharing efforts, should bring these new organizations into the effort, provide exposure to others with similar challenges, and help to bring their value to the operators. In addition, DoD CIO can use lessons learned in this effort to guide information sharing policy for the Department.

The purpose of the DoD CIO efforts in Operational Information Sharing is to bring the information advantage to the defense operators. In the short term, this may require human intervention; in the long term, it should become more automated. The true measure of the success of Operational Informational Sharing is the proliferation of success stories, like those introduced at the beginning of this report, from just a few anecdotes to business as usual in DoD.

Appendix A, References

- [1] Defense Science Board 2006 Summer Study: Information Management for Net-Centric Operations Vol. I and Vol. II, April 2007
- [2] Department of Defense Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense", December 2, 2004
- [3] Department of Defense Information Management & Information Technology Strategic Plan 2008-2009
- [4] Department of Defense Information Sharing Strategy, May 4, 2007
- [5] Department of Defense Net-Centric Data Strategy, May 9, 2003
- [6] Department of Defense Net-Centric Services Strategy, May 4, 2007
- [7] Department of Defense Implementing the Net-Centric Data Strategy Progress and Compliance Report, September 14, 2006
- [8] Guidance for Implementing Net-Centric Data Sharing, DoD 8320.02-G, April 12, 2006

Appendix B, Results from Partner Efforts

The OIS Study team from the DoD CIO IP&I Directorate identified several candidate organizations that appeared to be executing aspects of Operational Information Sharing. The team approached each organization, with the prospect of providing “seed money” to the organizations; believing that the money might further help the organization perform additional work related to information sharing. In turn, the organizations would provide the OIS Study team with data, findings, and recommendations about the effort.

The DoD CIO team and each partner organization met to discuss the Operational Information Sharing vision and consider potential opportunities where the money could best be used. In several cases, the organizations already had plans that addressed aspects of operational information sharing, and with the seed money, these plans could be funded or accelerated. With agreement on the use of funds to support information sharing, the DoD CIO team worked closely with the partner organizations to establish a formal relationship. Each partner organization had a unique approach; therefore the Memorandums of Agreement (MOA), Military Interagency Procurement Requisitions (MIPR), Plans of Action & Milestones (POA&M) were tailored to reflect the respective approaches.

Defense Technical Information Center

The Defense Technical Information Center (DTIC) group invited the DoD CIO team to the DTIC facility in Fort Belvoir, VA to discuss the potential partnership. They were particularly interested in one capability within the OIS vision: an information broker available to the defense community, and specifically available to the operators within the combatant commands. At that time, DTIC was already planning to send an information broker to a PACOM exercise, Terminal Fury. Both teams determined the exercise would provide a rigorous assessment of how an information broker role might aid the COCOM staff with finding information and subject matter expertise from throughout the DoD community. The partnership would allow DTIC to expand the information brokering efforts across other COCOMs by assisting with the cost for travel and other related information broker expenditures.

Objective and Responsibilities

DTIC and the DoD CIO agreed on the following partnering objective:

Collaborate in order to assess the value of information brokering for the operator

Both teams desired to keep the roles and responsibilities simple, at a high level, and outlined the following roles and responsibilities:

DTIC shall:

1. Work to achieve the objective through its participation in a PACOM exercise, possible participation with additional combatant commands, activities to increase awareness among the combatant commands, and other activities in support of OIS.

2. Provide a Plan of Objective and Milestones for the OIS effort and provide periodic progress updates.
3. Provide bimonthly report on the usage of OIS funding.
4. Provide interim findings on the value of information brokering for the DoD CIO to use for FY09 planning.
5. Provide a final report that assesses the value of information brokering for the defense operator.

DoD CIO shall:

1. Provide DTIC with background on OIS objectives.
2. Collaborate with DTIC on planning.
3. Collaborate with DTIC on findings from the efforts.

Plan of Action & Milestones

The following DTIC POA&M provides the detail about tasks that DTIC established with the funds from the DoD CIO. To meet its responsibilities, DTIC's activities fell into two major categories. First, DTIC was able to participate in exercises with PACOM and USNORTHCOM. As shown in the POA&M, the support of the exercises included initial preparation, on-site participation, and reach back to DTIC and IAC services as needed during the exercise. Second, DTIC worked to increase awareness of its services among the COCOMs through briefings and conferences. The specifics of this are also detailed in the POA&M.

| Phase | Task/Item Description |
|---------------------------------------|---|
| Planning and Administration | |
| | Complete MOU |
| | Complete MIPR |
| | Develop POAM |
| | Bimonthly Funds Usage Report |
| | Complete MOA |
| | Complete MIPR |
| Participate in COCOM Exercises | |
| | Prepare gap research for PACOM Terminal Fury Exercise |
| | Exercise participation, DTIC Librarian at PACOM as member of S&T cell. Reach back support at DTIC |
| | MOU for next year's PACOM Terminal Fury exercise |
| | Prepare Gap Research for NORTHCOM exercise |
| | Exercise participation at NORTHCOM and reach back support at DTIC |
| | Briefed NORTHCOM on DTIC and IAC services |
| | Brief to DoD CIO re: participation in PACOM and NORTHCOM exercises 29 May 08 |
| COCOM Outreach | |
| | OIS e-mail to COCOM representatives to introduce DTIC and offerings |
| | Provided DTIC Overview at DLA COCOM Reps Conference |
| | Attended Defense Acquisition University Symposium |
| | JFCOM Partner e-mail |
| | Order collateral materials for OIS W/COCOMs |

| Phase | Task/Item Description |
|-------|---|
| | Exhibit and network at IED 2008 Symposium and EXPO |
| | Networked at Joint Program Executive Office for Chemical and Biological Defense, Washington, DC |
| | Site visit w/NORTHCOM and presented DTIC Overview |
| | Site visit w/JFCOM |
| | Exhibit and Network at Joint Warfighting Conference 2008, Virginia Beach, VA, |
| | Exhibit and network at Internal Soldier Systems Conference and Expo, Orlando, FL |
| | Participated in NORAD - NORTHCOM Panel to help integrate S&T |
| | Presented DTIC Overview at 2008 Pacific Operational S&T Conference & Expo, Hawaii |
| | Exhibit and network at 2008 Pacific Operational S&T Conference & Expo, Hawaii |
| | Order Promotional material for OIS W/COCOMS |
| | Site visit w/SOCOM and present DTIC Overview |
| | Site Visit w/CENTCOM and present DTIC Overview |
| | Exhibit and network at Naval S&T Conference |
| | Site visit with USSTRATCOM and present DTIC Overview |
| | Site visit with USSOCOM SOAL |
| | Site visit with USSOUTHCOM and present DTIC Overview |
| | Site visit with USAFRICOM for briefing & training |
| | Teleconference with JFCOM; KNIFE invited - present DTIC Overview |
| | Exhibit and network at Association of the U.S. Army Annual Meeting & Expo, Washington, DC |
| | PEO Workshop |
| | Provide Community Pages for COCOMS |
| | Develop COCOM Community Web sites with specific sites for each COCOM, starting with PACOM |
| | Purchase most appropriate database; provide on DTIC Online (Controlled Access) site; purchased Jane's |
| | TS Clearances |
| | 5 approved; documentation in process; |
| | Develop Findings |
| | Develop Interim Findings |
| | Develop Final Report |

Progress and Results

DTIC made significant progress working with COCOMS to expand the information broker vision, and provide education about the capabilities of DTIC. This section describes some of the specific results from DTIC OIS activities.

Information Broker at PACOM Exercise, April 2008

The DTIC reference librarian acted as an information broker during the PACOM exercise Terminal Fury providing on-site technical expertise and reach back capabilities. The librarian was provided a listing of issues prior to the exercise, which he and the DTIC team thoroughly researched. However, the information PACOM requested was for new innovative technologies and products instead of technical reports, therefore not all the advance research proved relevant.

The cell processed up to 20 taskers a day, supported by an indeterminate amount of searches. The taskers were given to the researchers verbally during the Commander's Update Brief (CUB) and by other cell members upon return from visiting other cells based upon observations. The librarian's contribution was deemed a success. For example, within the first four hours of the exercise, the cell exceeded the production of the prior year's cell for the entire exercise. The quad charts created by the librarian were used in every Commander's Update Briefing (CUB) to the Commander, Pacific Command.

A set of improvements suggested by the DTIC participants included: information broker must have TS/SCI Clearance as well as access to the SIPRNET and JWICS fabrics; the Information Analysis Centers (IAC) need to have SIPRNET capability; the logistics permitting two librarians would be more efficient; and, that a cell phone for the information broker would be helpful.

Information Broker at NORAD-USNORTHCOM Exercise, May 2008

The purpose of this USNORTHCOM activity was to exercise national capabilities to prepare and respond to multiple incidents, including natural disasters and terrorist incidents. The team was notified that there would be three major events: a category 4 hurricane on the east coast (D.C. area), a terrorist event (i.e., IED, VIED), and a chemical incident at a northwestern chemical depot (Umatilla). Additionally, the team was presented with two unplanned requests: a tunnel mitigation in the southwest, and drug detection technology (specifically to detect crystal methamphetamine). As in the PACOM exercise, an extensive amount of research and analysis was required, and additional time was required to provide information in an easily understood bibliographic format.

Regarding suggested improvements, the DTIC participant noted that having a more formalized process to produce and share the bibliographies of information they assembled would have added to the efficiency of the exercise. He also noted that DTIC's participation in the exercise greatly enhanced their understanding of the culture and needs of the COCOM during situations. The information broker provided value by his ability to sort through a vast amount of information and present it to requestors in a meaningful and useful manner.

COCOM Outreach

DTIC completed outreach to all COCOMS, which included site visits and briefings. The specific activities are noted in the POA&M. They also promoted their services to conferences including the IED Symposium & Exposition, and the Joint Warfighting Conference, and many other exhibitions. Of note, DTIC has started collaboration with another DoD CIO partner organization, KnIFE.

Moving Forward

For FY 2009, DTIC will continue their outreach and education activities to the COCOMS. They also are developing the Program Executive Officer (PEO)/Program Manager Symposium, aimed at DoD Acquisition community. The symposium is scheduled for Nov 2008, in Huntsville, AL, and will provide rapid research for scientific-technical acquisition. The symposium will improve PEO

awareness of information technology, identify critical issues in community, and promote availability of DTIC's broad range of online resources

Contact Information

<http://www.dtic.mil>

Knowledge and Information Fusion Exchange

The OIS Study team and Knowledge and Information Fusion Exchange (KnIFE) teams met at the KnIFE facility in Suffolk, VA to outline the partnership. KnIFE had completed a rapid development effort to deploy a website as DoD's foundational information brokerage and repository for IED defeat information and was now providing watch center support to DoD. KnIFE had already established a Cooperative Research and Development Agreement (CRADA) with Microsoft which provides no-cost, mutually beneficial experimental development of software and technology. KnIFE expressed interest in working with the DoD CIO to leverage information brokering activities and more rapidly expand the KnIFE capabilities.

Objective and Responsibilities

KnIFE and the DoD CIO agreed on the following partnering objective:

Collaborate in order to assess the effectiveness of the KnIFE information sharing model as the focus is broadened beyond the defeat of IEDs.

Both teams desired to keep the roles and responsibilities simple, at a high level and outlined the following roles and responsibilities:

KnIFE shall:

1. Work to achieve the objective through the expansion of its current capabilities to additional Asymmetric Warfare topic.
2. Provide a Plan of Objective and Milestones for the OIS effort and provide periodic progress updates to DoD CIO representatives.
3. Provide bi-monthly report on the usage of OIS funding.
4. Provide interim findings on the expansion of its current capability to additional tsks.
5. Provide a final report that assesses the ability to expand into additional asymmetric topic areas.

DoD CIO shall:

1. Provide KnIFE with background on OIS objectives.
2. Collaborate with KnIFE on planning.
3. Collaborate with KnIFE on findings from the efforts.
4. Provide \$160K of funding for contractor hours to facilitate KnIFE's support of OIS.

Plan of Action & Milestones

| Phase | Task/Item Description |
|--|---|
| Planning and Administration | |
| | Complete MOA |
| | Complete MIPR |
| | Develop POA&M |
| | Financial Report |
| | Provide periodic updates on topic implementation plan |
| Plan Topic Expansion | |
| | Determine Asymmetric Warfare topics for inclusion |
| | Provide periodic updates on topic implementation plan |
| | Expanded survey |
| Develop and Deploy Broadened Topic Area | |
| | Design initial IW Site for KnIFE portal |
| | Initial data collection for IW site |
| | Roll out Topics 1, 2, and 3 |
| | Collect metrics for Topics 1, 2, and 3 |
| Develop Findings | |
| | Interim findings report |
| | Site usage metrics report |
| | Develop final report |

Progress and Results

KnIFE established a forward facing Sniper web portal on August 21, 2008 and broadened its core IED product to include related subjects such as combined/complex attacks, suicide bombers, and related material.

KnIFE worked in an agile development environment and was able to quickly leverage lessons learned. For example, the initial topics they anticipated covering with the seed money were Sniper, Suicide, and Complex Attacks. However, as they developed and deployed the Sniper site, they found that establishing separate sites for Suicide and Complex attacks was redundant with their existing IED defeat site. KnIFE therefore rolled the extra effort into developing the information and posting that on the existing site, and importantly -- will be able to maintain this capability for the remainder of the FY with money already received. It is important to maintain this content so they can continue to measure the use, effect, and other factors over a meaningful period of time.

During the first month of use, the KnIFE Sniper site showed considerable use, noted in the following charts.

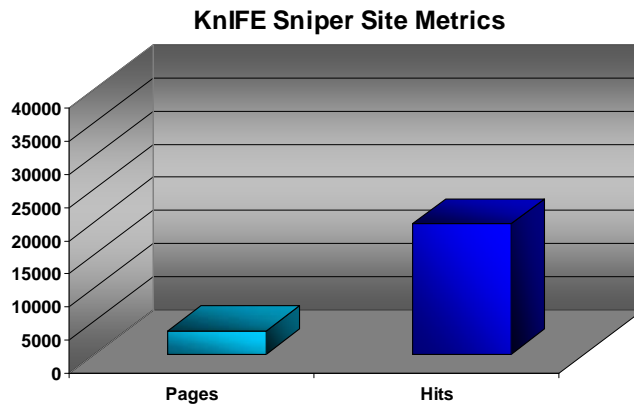


Figure A- 1, Number of Pages and Hits for September 2008

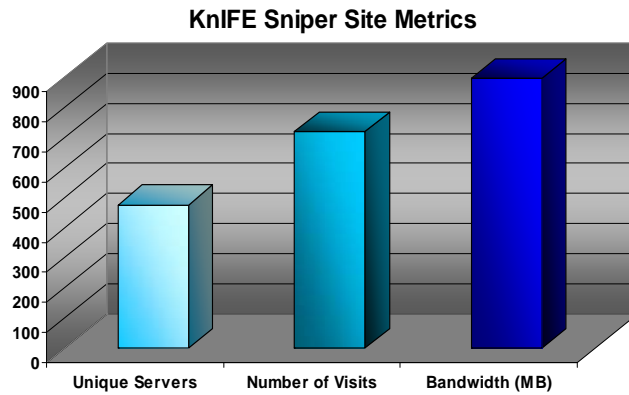


Figure A- 2, Number of Unique Servers, Visits, and Downloaded Bandwidth, Sept 2008

After four months, activity on the Sniper site continues to be significant as shown below:

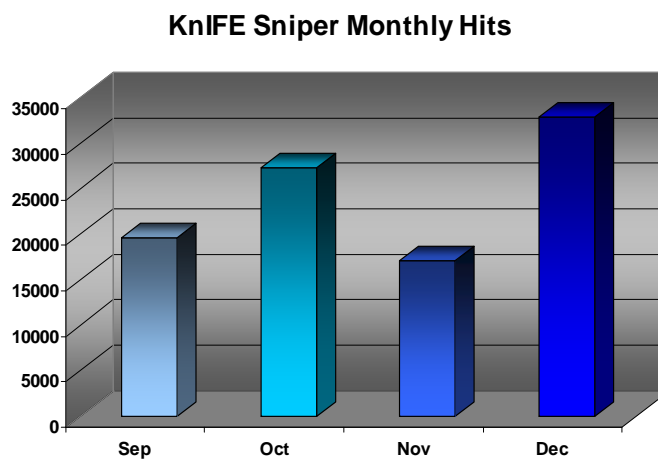


Figure A- 3, Number of Hits from Sept to Dec 2008

Moving Forward

KnIFE plans to expand to the operational and strategic level by including two additional subject areas. One of the likely areas of expansion is “threat finance”. Illicit finance facilitates recruitment of individuals, procurement of material, emplacement of IEDs, and other asymmetric tactics employed by insurgents. KnIFE started gathering sources of information from an international array of organizations.

KnIFE is collaborating with the DTIC reach-back librarians and leveraging the DTIC COCOM work, where KnIFE hopes to gather more information for sources of input to the growth of their capabilities.

Contact Information

<http://KnIFERFIwatch.jfcom.smil.mil>

Intelligence Community Enterprise Solutions

The DoD CIO team visited the Intelligence Community Enterprise Solutions (ICES) team in Annapolis Junction, MD, early in their partner selections. They saw the ICES Intelink help desk in action and learned more about the background and history of the project. ICES explained that several of the Intelink capabilities were in a transition phase, based on user visits and usage, e.g. blogs were emerging as one of the most heavily used services. Intelink was working closely with the Google suite of products, tailoring them as necessary.

Objective and Responsibilities

ICES and the DoD CIO agreed on the following partnering objective:

Collaborate in order to:

- *Support and encourage use of information sharing tools and techniques by operators*
- *Develop and assess methods of measuring information sharing activity by operators*

Both teams desired to keep the roles and responsibilities simple and at a high level and outlined the following roles and responsibilities:

ICES Shall:

1. Work to achieve the objectives through supporting and monitoring information sharing activity of Combatant Command staff, and by assessing methods and tools for measurement of the information sharing activity.
2. Provide a Plan of Objective and Milestones for the OIS effort and provide periodic progress updates to DoD CIO representative.
3. Provide bimonthly report on the usage of OIS funding.
4. Provide interim findings on the measurement of information sharing activity for the DoD CIO to use for FY09 planning.
5. Provide a final report that assesses the ability to measure information sharing activity

DoD CIO shall:

1. Provide ICES with background on OIS objectives.
2. Collaborate with ICES on planning.
3. Collaborate with ICES on findings from the efforts.
4. Provide funding to ICES in support of OIS.

Plan of Action & Milestones

| Phase | Task/Item Description |
|------------------------------------|--|
| Planning and Administration | |
| | ICES Kickoff Meeting |
| | Complete ICES MOU |
| | Complete ICES MIPR |
| | Develop ICES POAM |
| | Approve ICES POAM |
| COCOM Survey | |
| | Existing Study Survey & Review |
| | Focused Survey Preparation & Reporting |
| | Review initial results and guide adjustments as needed |
| | Expand Survey |
| | Stop Survey Collection |
| | Develop Survey Findings & Results |

Progress and Results

The DNI/CIO/ICES office prepared an automated survey to assist with gathering information on how people use social software. This survey was placed on SIPRNet using a MyPages survey tool and announced on Intelink Central. Key personnel in the three focus commands, STRATCOM, PACOM, EUCOM, were contacted and a notice was set within their organizations to encourage participation. We did not limit the survey to only the three stated commands but allowed anyone to participate and provide feedback.

Intelligence Community Enterprise Solutions (ICES) has provided the Intelligence Community and DoD, enterprise web services since 1994. These web services are commonly known to the community under the brand name of “Intelink”. In the responses from the survey you will see both Intelink services and ICES services referenced. They are one and the same.

Goals of the Survey

- To foster DoD (PACOM, STRATCOM, EUCOM) use of the DNI/ICES collaborative tools suite on the SIPRNet fabric.
- To better understanding how people currently use information sharing technologies such as Intellipedia (wikis), blogs, Inteldocs, bookmarks (TagConnect).
- To assess the potential benefits of information sharing functions and see how they can be applied to the war fighter.

Methodology

Our methodology consisted of a fourteen question on-line survey. Some questions provided pick-lists options. Free text responses were allowed in an effort to collect stories on how individuals utilize the enterprise tools. A variety of notification methods were utilized.

1. E-mail notification was sent to primary POC's at PACOM, EUCOM, and STRATCOM. These COCOM POC's selected a number of individuals that they encouraged to fill out the survey.
2. A Survey Announcement was made on the SIPRNet Intelink Central page inviting anyone to participate.
3. A SIPRNet blog entry was made to announce the survey.

Dates of Survey

August 1, 2008 thru September 30, 2008

Summary of Survey Responses

The survey had 148 responses as of 30 September when the survey was stopped. The participation by command was:

- PACOM -- 37% of responders
- STRATCOM -- 19% of responders
- EUCOM -- 13% of responders
- Other survey participants -- 30% of responders

For the questions that can be summarized, here are the responses. To see the best of the individual responses to the survey questions, please see

1. What is your role in the intelligence cycle?

Most respondents were Analysts (38%) or Consumers (28%). Two Watch Officers replied and Nineteen management personnel replied.

2. Does your job primarily involve working independently or do you regularly work in groups?

Responses were evenly split between group and independent working environments.

3. Which Combatant Command are you currently supporting?

PACOM: (55 responders)

STRATCOM: (28 responders)

EUCOM: (20 responders)

Other: (45 responders)

4. Which organization do you operate in on a daily basis?

- Responders covered all of the options provided (J2-6 and other)

- 52% operate in J2, 16% in J3 and the remaining responders evenly scattered within the reply options.

5. Who do you consider to be your primary customer?

- Most survey responders consider J2 to be their primary customer but a surprising number of “Other” responders to the survey indicated that Tactical
- War Fighters were their primary customer.
- The responses by COCOM were:

| COCOM | J2 | J3 | Policy Maker | Tactical Warfighter | Other |
|----------|----|----|--------------|---------------------|-------|
| PACOM | 22 | 15 | 5 | 6 | 3 |
| STRATCOM | 6 | 6 | 7 | 0 | 3 |
| EUCOM | 9 | 4 | 3 | 3 | 1 |
| Other | 5 | 7 | 5 | 15 | 11 |

6. Which of the following do you regularly use?

Intelink search was by far the most frequently used service, followed by Intellipedia. White pages (locator) and Inteldocs (document storage) came in third and fourth as the most used services

7. Which of the above tools are the most useful to you?

The overwhelming response was search. It appears that there is still a need for training on how best to use the search engine.

8. Outside of work which of the following do you use regularly?

Wikipedia is by far the most widely used tool outside of work by all commands surveyed. YouTube is the second most widely used tool.

Contact Information

<http://www.intelink.gov>