

Climbing the Knowledge Management Mountain

Lessons Learned from Operation Blinding Storm



By Cmdr. Kathy Donovan and Lt. Cmdr. Danelle Barrett

Introduction

New collaborative tools and cross-domain technologies being introduced to the fleet are presenting knowledge managers with exciting opportunities and significant challenges. These tools are the means to achieve new levels of operational efficacy, efficiency and interoperability, but users must incorporate process changes to gain maximum advantage. Knowledge managers must find ways to ensure users understand and embrace these capabilities by making the introduction of new technology relevant, quick and easy.

The following definitions are provided to ensure an understanding of the terms used in this article. Knowledge management (KM), as defined by Karl-Erik Sveiby, "is the art of creating value from intangible assets." Sveiby states that knowledge management aims to direct the ways in which we create, discover, exploit, disseminate and retain the expertise, understanding and practical know-how that individuals and organizations possess. (This information is available on Sveiby's Web site at <http://www.sveiby.com/>.)

In Navy terms, we interpret a knowledge manager as someone who obtains and analyzes information, sorts out what is needed, how it will be evaluated in operational context and used by operators. Operators use "know-what" and "know-how" to gain tacit knowledge and wisdom as depicted in Figure 1. This knowledge becomes a decision point for the commander.

Background

In the context of a Carrier Strike Group (CSG) we define information management (IM) as the understanding of the operational environment coupled with technology and command and control, communications, computers and intelligence (C4I). IM is a convergence of the tools, processes and procedures to expedite data, information flow and analysis.

Commander, Cruiser-Destroyer 8 (COMCRUDESGRU 8) participated in Combined Joint Task Force Exercise (CJTFFEX) 04-2, Operation Blinding Storm, as the Combined Forces Maritime Component Commander (CFMCC) aboard USS Mount Whitney (LCC 20), May 21 - June 21, 2004.

This exercise introduced new tools to improve IM and KM: cross-domain chat, Web replication between network enclaves and cross-domain mail guards. (See the IM Sample Toolkit on page 31 for more information.) More importantly, it provided opportunities for operators to change processes to leverage technologies to full potential — opportunities which were met with varying degrees of success.

During CJTFFEX 04-2, the CFMCC reported directly to the Combined Joint Task Force Commander – Commander, Second Fleet. As an afloat CFMCC, our staff was responsible for operational control of five Subordinate Maritime Commanders (SMCs) including the USS

Know what -
Raw material for decision making

Know how -
Resources required to act effectively

Facts	Beliefs
• List of who knows what	• Assumptions – mental models
• Concepts, theories	• Values, attitudes
• Data on sales, costs, markets, etc.	• Common sense
Procedures and Rules	Attitudes
• Assumptions – mental models	• Expertise/artistry
• How-to manuals	• Learned behaviors
• Automated processes	• Culture
• Contingency plans	• Body Skills
• Methodologies	• Intuition

Information - Structured and coded

Tacit Knowledge - Unstructured, not coded

Figure 1. Karl-Erik Sveiby's Internal Knowledge Resources

John F. Kennedy (CV 76) CSG; USS Harry S. Truman (CVN 75) CSG; HMS Invincible Task Group; Commander, Mine Warfare Command; and the Maritime Patrol and Reconnaissance Aircraft Group under the direction of the Canadian Air Division Commander Maritime Air Commander Atlantic.

The maritime coalition consisted of 60 ships and 200 aircraft from the United States, Canada, United Kingdom, Germany and Peru. The challenges from an interoperability and KM perspective were immediately apparent.

✓ How could the coalition forces exchange knowledge and information rapidly and securely in a bandwidth disadvantaged environment?

✓ What set of common collaborative tools existed to communicate?

✓ How could users be quickly registered and indoctrinated to the new tools, including the cross-domain chat, secure mail guards and document sharing via Collaboration at Sea II?

✓ How could existing tactics, techniques and procedures be improved using the new tools?

The KM Mountain

The tools and people are in place, the summit is within view, how then does the knowledge manager facilitate the users leap to the top?

First and foremost, an organizational understanding and acceptance must take place. Specifically, that KM is not an N6 or techie function — it is a process that belongs to everyone with the knowledge manager serving as the lead change agent. True KM and its ultimate by-product, wisdom, do not occur in a vacuum. There must be an

alignment across the organization and its key functional areas. On a Strike Group staff this would include N2 (Intelligence), N3 (Operations) and N6 (Communications). Without proper alignment, the sum of the parts will never exceed the whole — and the potential exists for inefficiencies, stovepipes within departments or poor operational choices.

The knowledge manager instructs users about KM practices and its subset IM. By encouraging and fostering an understanding of these concepts, people can begin to re-evaluate existing tactics, techniques and procedures (TTP) with the goal of shared tacit and implicit information. Tools that are cumbersome or confusing are quickly abandoned. The knowledge manager can facilitate by: Making tools easy to register for, understand, use and leverage. For users, a process should be reengineered and technology applied (best scenario) or an existing process can be used with a new technology (the least desirable scenario).

There was both KM success and failure during Operation Blinding Storm. A success was the Second Fleet Knowledge Management Board, chaired by the Canadian Navy Deputy Chief of Staff for Commander, Striking Fleet Atlantic, Capt. James T. Heath. The board was attended by key stakeholders from every department and executive agents from the public affairs offices, flag staffs and component commanders' liaison officers (LNOs). Using standard operating procedures, the board worked on the process piece, the most important and challenging aspect of KM.

Within the CFMCC, the human element was the area that required the most improvement. While there were many new tools available, most people reverted to old processes using new tools rather than changing the process to leverage new tools to advantage. A lot of time was spent pushing information, but not a lot of time was spent analyzing and taking action. In short, there was too much time spent on the output and not enough time on the outcome.

To counter this process problem, all cells within the CFMCC should have a full-time, trained knowledge manager — a “power user” — someone experienced in information technology, who also has operational understanding to ensure information is shared for timely decision making. Although the watchbill included a knowledge manager for every watch section, this function was not clearly understood. People assigned quickly became tasked with other work, and the KM function was perceived as a collateral duty.

The elements of KM, and even basic elements of IM, fell by the wayside as people reverted to known processes and methods for sharing information and knowledge. CFMCC knowledge management cells sprouted like mushrooms when there was an information crisis and dissipated as the crisis went away.

The CFMCC knowledge management successes realized were not necessarily orchestrated, rather they emerged. As the tools and processes associated with IM and KM become well understood throughout the fleet, important lessons can be learned and shared.

The following are several lessons learned that resulted from our experience in Operation Blinding Storm that are applicable on the Carrier Strike Group level.

✓ The knowledge manager should be a special assistant to the chief of staff (COS). While the function of knowledge manager relies heavily on the tools and paths provided by N6, KM is not inherently or solely an N6 function. Rather, it cuts across all disciplines within a Strike Group from operations and logistics to force protection and administration.

✓ The COS should chair the KM Board. The COS is in the best position to ensure a process is instituted for evaluating data and providing analytical information to the commander.

✓ Everyone must understand that KM is a critical element of any staff and must be built into the battle rhythm.

✓ Each ship in the CSG should designate, at a minimum, a khaki level N3 and N6 representative to actively participate on the board.

✓ Prior to CSG work-ups, group sails and deployment, the KM Board must have high priority with an updated KM Plan and IM Matrix that are understood and tested in C4I Fast Cruises. The cruises should test capabilities, tools and processes to ensure that the most effective tools are used during actual operations. If the plan is formulated prior to group sails with all key stakeholders, then bandwidth limitation issues can be resolved resulting in real process improvement.

✓ As the CSG deploys, the KM Board should meet frequently, virtually and in a collaborative environment when possible and face-to-face communications are impractical or unnecessary. At a minimum, the board should collaborate prior to entering a new theater of operations, so unique requirements are understood and solutions are leveraged throughout the CSG. This allows the group to be more proactive using strategic planning rather than reacting to the latest information crisis.

The KM lessons learned from Operation Blinding Storm are common and practical suggestions. While much can be shared in terms of lessons learned, it is a mistake to think that any one KM Plan or Navy-Wide OPTASK Information Management Plan will be a one-size-fits-all solution.

This type of plan is beneficial for overarching guidance and recommendations where standardization is realistic operationally or technically. However, each theater and each situation has unique knowledge requirements that must be considered, such as joint and coalition requirements, availability of IM tools, information assurance and foreign disclosure issues, etc.

KM is in its infancy in the Navy. It can be challenging to organize, but with proper tools, training and process improvements it can be an empowering force enabler. The summit can be reached and success achieved through proliferation of appropriate IM tools and iterative Navy-wide training.

One suggestion is that the resource sponsors of the major communities within the Navy could ensure KM training is integrated into all warfighting and supporting disciplines — not just as a stand-alone topic. Training included in every level of tactical instruction for officers and enlisted will instill a sense of process ownership from Sailor to Admiral.

Information Management Sample Toolkit Operation Blinding Storm

The following are the technologies we worked with in Operation Blinding Storm and our evaluation of their effectiveness. The first step in discerning the effectiveness of operational tools is to look at their capabilities and concepts.

[Cross-domain Secure Mail Guards](#). This technology has been around for several years, but the fleet is just beginning to use it. An example of the mail guards used in Operation Blinding Storm were: (1) Secure mail guard at COMUSNAVEUR connecting the SIPRNET and the classified United Kingdom national network Combat Support Systems (CSS); (2) Pacific Region Network Operations Center connecting SIPRNET with the Combined Enterprise Regional Information Exchange System (CENTRIXS) Four-Eyes (United Kingdom, United States, Canada and Australia); and (3) Global Reach Interactive Fully Functional Information Network (GRIFFIN) connecting SIPRNET to several other nations' national classified systems.

As e-mail passes through the guards, messages are screened for a classification line at the top, embedded malicious code, and inappropriate or unauthorized words that may result in an inadvertent disclosure of classified information. If the format line is incorrect or an unauthorized word is discovered, the message is rejected and returned to the user. Many of these guards allow e-mail attachments, and this capability proved extremely successful in aiding information flow. Most of the difficulties encountered with the guards were process not technology based. The registration process can be cumbersome, errors in the classification line (which causes the message to be rejected) are common, and the inappropriate words lists were not readily available, so users did not always know why an e-mail was rejected. Users were also confused by the different guards and the unique e-mail address associated with each guard.

The CFMCC N6 staff assisted users with registration, and we loaded Classify software, which preconfigures mail guard classification line options for users to choose from. Having a drop down menu of options with clear guard titles reduced the occurrence of human error. This was particularly important because there were five different mail guard options, each with different classification line requirements. Users who didn't learn how to use the guards were quickly frustrated with their inability to move information easily.

[Multi-Level Secure Chat](#). This program, developed by the Naval Research Laboratory and the Naval Warfare Development Center, was beta tested during the exercise. It allowed operators to chat between the CENTRIXS Four-Eyes and SIPRNET enclaves. The program provided user authentication, an important security feature in any chat tool, and a necessity as chat becomes more acceptable for passing tactical information and orders.

From a user perspective, this tool had several attractive features, such as the ability to view the discussion that preceded the user joining

the chat room. This is important for maintaining situational awareness for afloat units which frequently lose satellite connectivity and need to rejoin a discussion. Another great feature was that this tool allowed U.S. watchstanders to remain at their SIPRNET workstations rather than move to CENTRIXS workstations, which were limited in number and not located in spaces where key staff members operated.

A follow-on goal could be to expand this tool between national systems. Development of the tool should continue as a Web service and be integrated into the shared infrastructure of the Fleet Application Server. While the program is based on homegrown proprietary code, giving the code to the open source community for further development could yield big results at little cost. Additionally, the program should be tested by the Joint Interoperability Test Command for inclusion into the Defense Collaborative Tool Set.

[Cross-Domain Replication](#). Document sharing was facilitated using the IBM Lotus Domino based Collaboration at Sea (CAS) II on CENTRIXS and SIPRNET. Cross-domain replication, enabled by the Pacific Region Network Operations Center, assisted in this capability. CAS has been used successfully for several years, but a new feature was added during Operation Blinding Storm — users could post information on the CAS II Web site hosted on both SIPRNET and CENTRIXS Four-Eyes. The CAS architecture presents an excellent way to smartly replicate change only data in a discontinuous, bandwidth disadvantaged environment.

The Operation Blinding Storm CAS II site, designed and maintained by Navy Cmdr. Paul Matheson from Second Fleet, was the central repository for information sharing between all component commanders and the CFMCC Subordinate Maritime Component Commanders. While this tool presented a leap in cross-domain information sharing, lessons learned included: (1) Lengthy replication times between domains (three hours to several days); (2) Shipboard Web browsers had to point to the server afloat to conserve bandwidth; (3) Training was needed for posting and retrieving information, registration and avoiding replication collisions.

Solving these problems involves both technology and process changes. Latency issues could be mitigated by hosting servers at the Unified Atlantic Region Network Operations Center and the Naval Computer and Telecommunications Area Master Station, Naples, which could replicate and synchronize databases at the primary point of presence locations for afloat units. Information managers could help users by working with CAS II developers to create a tool to mass register users of deployed afloat commands traveling from one server to another (i.e., COMCRUDESGRU Eight to Second Fleet to USS Harry S. Truman).

Information managers could also develop a way to prioritize replication for smaller files first, and integrate a notification capability that would inform users of updates to specific sections of Web sites they subscribe to.

Cmdr. Donovan and Lt. Cmdr. Barrett are Information Professional Officers assigned to Commander, Cruiser-Destroyer Group 8. Cmdr. Donovan is the Deputy N6 (C4/IW) Officer and Barrett is the Communications Officer.