9th International Command and Control Research and Technology Symposium

Coalition Transformation: An Evolution of People, Processes, and Technology to Enhance Interoperability

Topic: C2 Experimentation

Title: Human Systems Integration Assessment of Network Centric Command and Control

Authors:
Dee Quashnock, Space and Naval Systems Command;
Richard T. Kelly, Pacific Science and Engineering;
John Dunaway, Antin, Incorporated;
Robert J. Smillie, Space and Naval Warfare Systems Command

Point of Contact: Robert J. Smillie, Ph D, CPE
Deputy Director
Human Systems Integration Department
Space and Naval Warfare Systems Command
4301 Pacific Highway
San Diego, CA 92110-3127

Phone: 858-537-8886
FAX: 619-553-9391
email: robert.smillie@navy.mil

ABSTRACT. Trident Warrior 2003 (TW03) was a Navy initiative to demonstrate an initial baseline of potential FORCEnet capabilities. FORCEnet is the operational construct and architectural framework for Naval Network Centric Warfare in the information age that integrates warriors, sensors, networks, command and control, platforms, and weapons into a distributed combat force. TW03 provided an integrated prototype capability for fleet evaluation and refinement of a supportable incremental delivery of FORCEnet capability. The Chat system was limited by the synchronous nature of the system that required constant attention to monitor communications, by the number of participants that could be accommodated and recognized, and by the time required for users to authorize, compose, and type messages. The connections between the fire control systems allowed users to share common situation awareness on tracks, targets, and fire schedules but were mediated by the GCCS-M position information, which could lag up to 15 minutes behind real-time. The utility of the links between the fire support systems were limited by the inability of one system to accommodate the same target designations from another system and by the lack of connection between systems. Situation awareness is a continuing process and the limitation of reliance on chat as a status indicator was highlighted when one shooter was not aware that he was supposed to be in position to provide fire support to shore. Chat technology was used extensively to transfer information among distributed teams. Confusions and missed messages were noted occasionally and were typically due to user interface design problems, ambiguous operating procedures, or technical incompatibilities between chat systems. Display configurations and workspace layouts were problematic and led to inefficiencies in the way that information was transferred within and between command centers. Consideration of the proper location of operator workstations, legibility of shared displays, and easy access to task-relevant information would improve operations. While training was available on how to operate individual FORCEnet systems, little instruction was provided concerning how to employ the systems for maximal operational effectiveness. eated insufficient manpower for the new systems, limited their usefulness and adaptability. HSI is an important consideration in FORCEnet systems analysis and assessment. FORCEnet systems rely upon the performance of human operators and/or maintainers, despite their level of automation. Therefore, HSI issues need to be examined along with the technical aspects of the systems themselves as part of the total systems engineering approach.

INTRODUCTION. Trident Warrior 2003 (TW03) was a Navy initiative to demonstrate an initial baseline of potential FORCEnet capabilities. FORCEnet is the operational construct and architectural framework for Naval Network Centric Warfare in the information age that integrates warriors, sensors, networks, command and control, platforms, and weapons into a distributed combat force. TW03 provided an integrated prototype capability for fleet evaluation and refinement of a supportable incremental delivery of FORCEnet capability.

The TW03 FORCEnet capabilities supported operational objectives in the following areas:

(a) Expeditionary, multi-tiered weapon and sensor information (Call For Fires),

(b) Distributed, collaborative command and control (C2 / Collaboration), and

(c) Dynamic, multi-path and survivable networks (Network Operations).

This paper presents major HSI issues that were identified through the analysis of field performance data.

FORCENET PROCESSES AND TECHNOLOGIES

Call For Fires. Call For Fires furnished a context for assessing the new form of C2 advocated by FORCEnet. Call For Fires entails a coordinated effort to identify, validate, and verify a potential target for fire. A major concern during Call For Fires activities is to confirm that the target is hostile, so as to prevent friendly fire casualties. To achieve its objectives, Call For Fires requires the coordinated use of three technologies: Automated Deep Operations Coordination System (ADOCS), Advanced Field Artillery Tactical Data System (AFATDS), and Naval Fire Control System (NFCS).

Command and Control/Collaboration. Command and control was integral to all TW03 activities. It consisted of capabilities that facilitated decision making, such as acquiring and maintaining situation awareness and a common operational picture. Collaboration enables the sharing of information among persons working on a common task or project. The collaborative technologies implemented for TW03 were intended to supply real-time communication among geographically separated individuals and groups. Several technologies were used that enabled participants to acquire and maintain a shared awareness of the battlespace: FORCEview, Global Command and Control System–Maritime (GCCS-M), Task Force Web (TFW), Web Common Operational Picture (WebCOP), and Collaboration Tools (Chat and MS NetMeeting)

Network Operations. Network Operations refer to establishing, operating, and maintaining information technology (IT) networks that support the activities of TW03. Hardware is the primary focus of Network Operations; the four technologies that were used during TW03 – Automated Digital Network Switch (ADNS), HF ALE, Intra-Battle Group Wireless Network (IBGWN), and Super High Frequency / Commercial Wideband Satellite Program (SHF/CWSP) – did not require ongoing user input. Information management personnel monitored the networks and serviced them as needed throughout TW03. The Network Operations data collected during TW03 centered on two activities: bringing the technology online and maintaining its function.

HUMAN SYSTEMS INTEGRATION (HSI) IN NAVAL OPERATIONS. HSI is a comprehensive management and technical strategy to integrate human considerations early in the

system design, development, and demonstration process. HSI plays an important role in efforts to create systems that accommodate human sensory, perceptual, cognitive, and physical performance characteristics. Its major goals are to improve total system performance and reduce costs of ownership.[1] Failure to take HSI into account during system design and implementation typically results in systems that are difficult to learn and operate reliably and efficiently. HSI accomplishes its goals by considering seven elements associated with system design, development, and implementation: manpower, personnel, training, human factors engineering, safety, health hazards, and survivability. Together, these elements define how human users affect a system (in terms of effectiveness, operation, and support and their associated costs) and how a system affects the humans who interact with it (e.g., operators, maintainers, supporters, trainers). Although each element is important, Human Factors Engineering has primary responsibility for establishing HSI human performance objectives, thresholds, and characteristics. This, plus manpower, personnel, and training, are the primary areas of HSI analysis for IT systems, such as FORCEnet.

FOCUS AREAS FOR HSI ANALYSIS. In order to assess the three FORCEnet processes (Call For Fires; C2 / Collaboration; Network Operations) and their component technologies during TW03, it is necessary to define HSI analysis goals.

An overarching goal of the HSI assessment in TW03 was to improve the kill chain. Technology and the warfighter are the two major elements in the kill chain that provide the greatest opportunity to accelerate the decision and fire control process from the initial stages of target detection to follow-up damage assessments. Improving the kill chain depends on effective HSI among FORCEnet capabilities and improved organizational processes and procedures. Four areas have been identified as primary attributes of warfighting effectiveness and served as focus areas for HSI analysis in TW03:

- **Shared Awareness**. A common perception and understanding of the tactical battlespace and of the roles, responsibilities, and actions of other warfighters.
- **Efficiency of Asset Utilization**. Length of time needed to assign an asset, time needed to complete a mission, number of tasks accomplished.
- **Speed of Command**. Time from when an event occurred until the ordered action was completed.
- **Adaptability**. The extent and speed of an organization's change in response to changing tactical situations.

To define these warfighting attributes in terms of human performance variables that could be measured during TW03, five HSI analytic elements were used:

- **Performance**. The performance variable assessed shared awareness and speed of command. Performance evaluations were based on three types of performance data

[1] Department of Defense (January 2001). *Glossary: Defense Acquisition Acronyms and Terms* (10th ed.). Department of Defense, Defense Systems Management College. Fort Belvoir, VA.

collected from TW03 participants during and after task performance: situation awareness, accuracy, and latency (time to perform).

- **User interface**. Experienced human factors usability analysts conducted user interface evaluations based on human factors usability heuristics. These evaluations supplemented the performance-based data with more detailed analytic information. The results of these evaluations are relevant to efficiency of asset utilization, shared awareness, and speed of command.
- **Information transfer**. The extent to which information needed to operate each technology in its intended manner as well as to achieve mission goals was assessed. This variable is related to shared awareness and speed of command.
- **Training**. Training assessments were performed to determine the type and extent of instruction needed to operate each technology effectively, efficiently, and safely; training is primarily related to adaptability to changing conditions.
- **Manpower and personnel**. Manpower and personnel requirements for the proper operation and maintenance of each technology were determined to the extent possible during TW03. This variable is primarily related to efficiency of asset utilization.

Together, these five HSI elements furnished the foundation needed to formulate and implement an analytic plan that enabled meaningful HSI assessments of the technological systems used during TW03 in support of FORCEnet objectives.

ASSESSMENT OF HSI PROCESSES. HSI observers were embarked onboard two ships as part of an Expeditionary Strike Group (ESG) prior to and during TW03. They collected data during key events related to (a) expeditionary, multi-tiered weapon and sensor information in the 'call-for-fire' process, (b) distributed, collaborative command and control, and (c) dynamic, multi-path and survivable networks.

HSI data were collected using a range of methods, including questionnaire ratings by FORCEnet users, interviews with operators, observations by HSI experts of operational performance and system administration, training effectiveness analysis, and usability analyses of FORCEnet software and workspace ergonomics.

HSI FINDINGS. The following table summarizes the FORCEnet operational processes analyzed during Trident Warrior 2003 in terms of major elements in Human Systems Integration (HSI)[2]:

HSI Process	HSI Element				
	Performance	User Interface	Information Transfer	Training	Manpower & Personnel
Call For Fires	G	G	Y	Y	Y
C2 / Collaboration	Y	Y	Y	Y	G
Network Operations	G			Y	

DISCUSSION. Individuals in the battle group are often isolated and must actively collect and share information to coordinate their actions. Coordination information was passed between distributed individuals via direct linkages between the fire support systems (ADOCS, AFATDS, NFCS, GCCS) and by way of collaboration tools (Chat, NetMeeting). The Chat system was limited by the synchronous nature of the system that required constant attention to monitor communications, by the number of participants that could be accommodated and recognized, and by the time required for users to authorize, compose, and type messages. The connections between the fire control systems allowed users to share common situation awareness on tracks, targets, and fire schedules but were mediated by the GCCS-M position information, which could lag up to 15 minutes behind real-time.

The utility of the links between the fire support systems were limited by the inability of AFATDS to accommodate the same target designations as ADOCS and by the lack of connection between the NFCS and the shooters weapon systems. These problems were circumvented by the operators who entered incorrect data into the systems that allowed the support systems to be used locally, but had the unfortunate result of sharing the incorrect data with other members of the CFF chain who then assumed that specified targets had not been engaged and issued redundant engagement orders.

Situation awareness is a continuing process and the limitation of reliance on chat as a status indicator was highlighted when one shooter was not aware that he was supposed to be in position to provide fire support to shore. Design of a tool that provides support to users in the form of process status indicators that augment the collaborative message content would help avoid some of these situation awareness problems.

---

[2] G Fully functional. Meets requirements but can be improved with minor modifications.
Y Functional but requires substantial modifications.
Inadequate data were available for valid assessment.

Chat technology was used extensively to transfer information among distributed teams. Confusions and missed messages were noted occasionally and were typically due to user interface design problems, ambiguous operating procedures, or technical incompatibilities between chat systems.

Display configurations and workspace layouts were problematic and led to inefficiencies in the way that information was transferred within and between command centers. Consideration of the proper location of operator workstations, legibility of shared displays, and easy access to task-relevant information would improve operations.

Engagement timelines for four CFF events have been reconstructed from ADOCS electronic logs, IRC chat logs and observer notes. The reconstructed timelines for these 4 CFF events show execution times from 31 to 230 minutes. The 230-minute response was a difficult target with high potential for collateral damage. But the timing suggests that the distributed CFF task performers did not realize that the window for engagement had passed or that a potential blue-on-blue situation might have occurred between the NLT and actual fires.

Another speed of command issue related to the information passed between members of the distributed fire support team was noted when the fire planning was completed and de-conflicted, but the TAO's involvement in adapting to a lost chat link prevented him from authorizing a pending CFF. The interconnections between the fire support systems (AFATDS-NFCS-ADOCS-GCCS) provided the potential to execute the fires scenarios much more safely and rapidly, but were not complete enough to pass all the information required to automate the CFF process (AFATDS did not recognize TGTD target nominations, and NFCS was not connected to the shooter's weapons).

While training was available on how to operate individual FORCEnet systems, little instruction was provided concerning how to employ the systems for maximal operational effectiveness. Because of the concurrent events during TW03, trained operators and maintainers were quite limited for most FORCEnet systems. This created insufficient manpower for the new systems, limited their usefulness and adaptability.

CONCLUSIONS. HSI is an important consideration in FORCEnet systems analysis and assessment. FORCEnet systems rely upon the performance of human operators and/or maintainers, despite their level of automation. Therefore, HSI issues need to be examined along with the technical aspects of the systems themselves as part of the total systems engineering approach. Specific HSI issues were identified for FORCEnet technologies and for their integration with legacy systems and procedures. Many of the FORCEnet technologies functioned well in TW03, but several areas for potential HSI enhancements were uncovered during the exercise.

Structured exercise test procedures are needed to permit collecting quantitative human performance data, including situation awareness, decision latency, and workload. HSI data collection and analysis was constrained by the diverse and often competing objectives of TW03, by the unstable introduction of scenario events / MSELs, and by the uncertainty about how the technologies would be used. Efforts to address these methodological issues earlier during exercise planning would permit much greater precision in the HSI data collected.