

## Perspectives and Trends

*Heide E. Heidepriem*

**T**he Joint Warfare Analysis Department (JWAD) helps the Laboratory and its sponsors to better understand the dynamic and evolving environment within which we function. One way that JWAD does this is through general background studies and assessments that provide perspective and a foundation for more focused endeavors. These studies are initiated in conjunction with current work for APL sponsors or in anticipation of sponsored work to better equip the Laboratory to serve those sponsors. This article describes how JWAD has performed this role for APL in a number of areas during the past decade and gives examples of the impact of our efforts. Highlighted are insights related to Desert Shield/Desert Storm and operations in Kosovo; Joint Warfighting Requirements and the increasing needs for combating terrorism; the emergence of the Infosphere and its military analog, Network-Centric Warfare; and an ongoing assessment of trends as part of the Laboratory's strategic planning. (Keywords: Analysis, Conflict, Military operations, Seminar, War room.)

### INTRODUCTION

An important role of the Joint Warfare Analysis Department (JWAD) is to assist the Laboratory and its sponsors to better understand the dynamic and evolving environment we all live in. In this role, JWAD endeavors to identify those areas in which APL can best apply its capabilities to enhancing the security and well-being of the nation.

The Laboratory and JWAD have initiated a number of studies and assessments during the past 10 years to develop perspectives and identify trends relevant to the mission and programs of APL. In some cases, these efforts were directly associated with the Laboratory's work for its sponsors. In other cases, they were in anticipation of sponsored work or indirectly related to

current efforts in that insights obtained would enhance the quality of work already being performed.

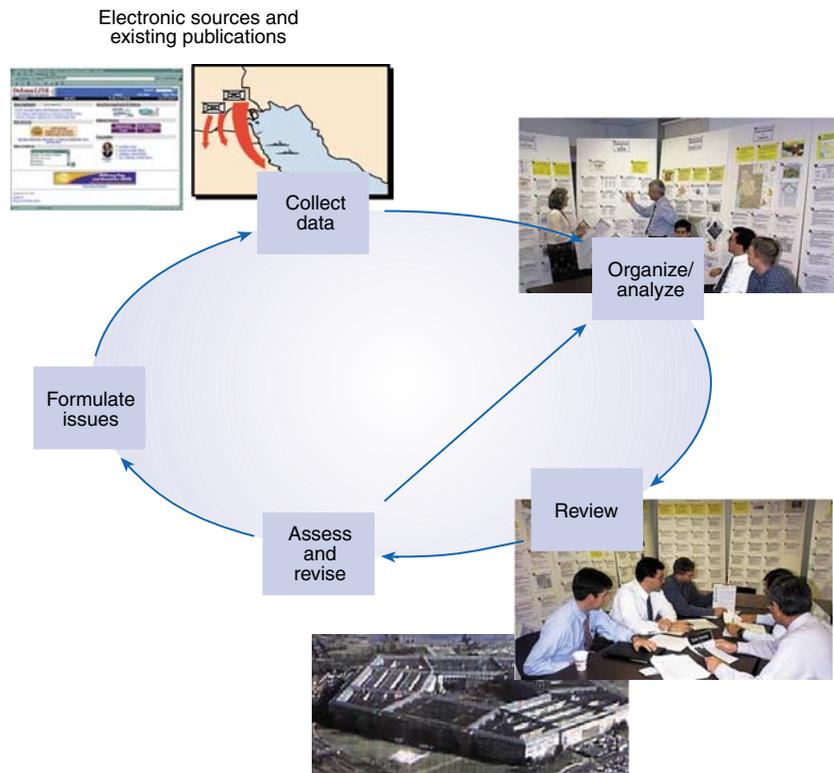
A variety of analytic methods have been used in these endeavors, including the establishment of study rooms (sometimes called "War Rooms"), seminar series, and Warfare Analysis Laboratory Exercises (WALEXs), as well as traditional forms of requirements and effectiveness analyses. This article focuses on the way that these initiatives contribute to the quality of warfare analysis at APL, with details about the methods left to others (see, e.g., the article by Sinex et al., this issue, which describes the War Room Process in more detail). Several articles in the previous issue of the *Technical Digest*, 21(2), described the Warfare Analysis

Laboratory (WAL), the WALEX Process, a variety of WALEX applications, etc. Most of the activities described in this article involve the establishment of a dedicated War Room and the use of an evolving process whose principal steps (Fig. 1) include the following:

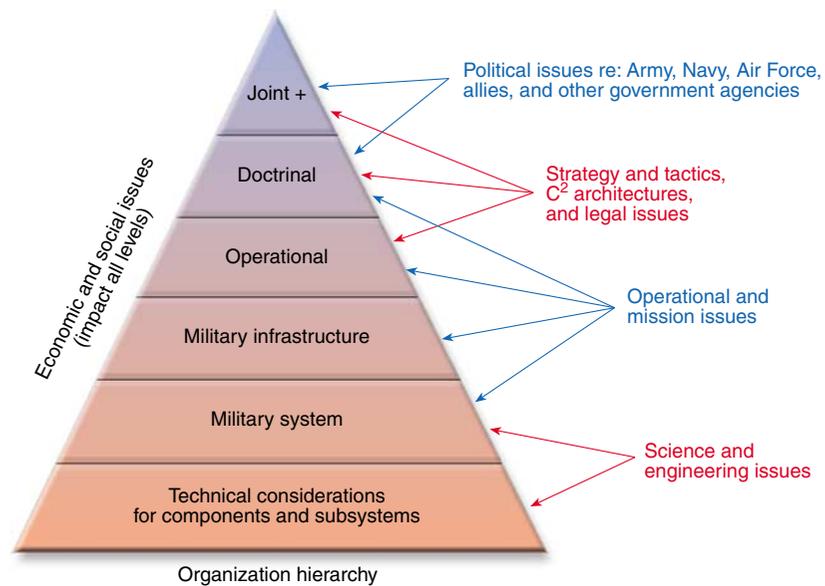
- Identifying and collecting information and data from a variety of disparate sources
- Organizing, summarizing, and analyzing these data to identify principal themes and to formulate issue statements
- Iteratively reviewing, revising, and adding new materials and perspectives gained from interactions with subject-matter experts and customers/stakeholders

A significant aspect of the multistep iterative process illustrated here is its potential to create coherence among the multiple perspectives that are brought to bear on a complex issue. Figure 2 illustrates how these perspectives must address the different levels at which a problem is viewed. These range from the microscopic, i.e., technical considerations (science and engineering details), to the macroscopic, i.e., Joint + (where differences in military structure and concepts among U.S. services, U.S. allies, and non-DoD branches of government must be accommodated). The orthogonal aspects of policy, social and legal considerations, and military practices must also be addressed across all of the hierarchical levels in Fig. 2. Coherence in addressing such complex factors means that the impact of one factor on another is considered and that assumptions related to each factor are compatible with assumptions for others. The iterative review, reassessment, and refocusing at the heart of the process described in this article is key to the development of such coherence in perspective.

Topical areas addressed here include military hostilities (e.g., Desert Shield/Desert Storm and



**Figure 1.** The multistep, iterative process applied within an APL "War Room."



**Figure 2.** Complex interrelationship of issues (C<sup>2</sup> = command and control).

Kosovo), evolving military requirements (e.g., Joint Warfighting Requirements and counterterrorism needs), emerging forms of Information Warfare (e.g., Infosphere concepts and Network-Centric Warfare), and the assessment of trends as part of the Laboratory's strategic planning. The article concludes with a look to the future and to other topics that may need to be addressed in a manner similar to those identified above.

## MILITARY HOSTILITIES

### Desert Shield/Desert Storm

As the confrontation with Iraq began to develop in late 1990, the Laboratory established a “Situation Room” in JWAD’s WAL to

1. Provide a central focus within the Laboratory for tracking and representing the daily events of the unfolding confrontation
2. Assemble, organize, display, and present relevant intelligence information as reflected in daily intelligence summary reports from the theater
3. Identify and assess emerging information about the threat, including “rest-of-world” threat systems as well as Iraqi innovations in integrating disparate systems and developing tactics to take advantage of these hybrid systems
4. Analyze selected environmental factors and engagement scenarios

This Situation Room helped the Laboratory to support its sponsors in identifying workarounds and tactics suited to addressing some of the perceived shortfalls of U.S. systems in this “new” and challenging environment and threat situation. Information developed for and reflected in the Situation Room included detailed material on threat systems and their unique characteristics and detailed and daily updated intelligence information on naval, air, missile, and electronic order of battle; deployment and employment of naval forces; and battle damage estimates during the extended air campaign.

During this period, the direct technical support provided by APL to many of its sponsors was enhanced by the more comprehensive appreciation of the operational environment that this Situation Room made possible. Several efforts were impacted in this way, included the EA-6B/EF-111 Electronic Warfare Program, Tomahawk Cruise Missile Program, Aegis Program, Standard Missile Program, etc. The Situation Room established in the WAL offered a Laboratory-wide forum for sharing information (and issues) pertinent to providing integrated technical support to our sponsors. Some representative topical investigations conducted in support of these events and contained in the Situation Room addressed

- Iraqi engineering innovations and their Integrated Air Defense System
- Gulf Region environmental summaries
- Mesoscale atmospheric modeling and predictions
- Anomalous radar propagation modeling and assessments
- Tomahawk mission planning and performance issues
- High-speed antiradiation missile effectiveness versus Iraqi systems

After Desert Storm was over, the threat assessments, environmental and operational databases, and technical performance assessments contained in the Situation Room were used to develop operational contexts and engagement situations (scenarios) for follow-on assessments of weapons and combat systems requirements for evolved and future systems. Even prior to more detailed follow-on studies and requirements analyses, several major technology and system development needs became clear through the Situation Room process and associated investigations (many of which are still high on the list of needs for our current and future military forces). These included the need for the fusion of multisource data; technology for locating, identifying, and targeting mobile targets; the ability to (quickly) locate, avoid, and neutralize sea mines; defenses against Tactical Ballistic Missiles; technology to allow full interoperability of Joint and combined forces; and technology to ensure electronic warfare effectiveness and responsiveness.

In addition to identifying principal technology needs evident from the Gulf campaign, JWAD analyzed these events to pinpoint important lessons learned from the Desert Shield/Desert Storm experience, both for the United States and its allies and from the perspective of future potential adversaries. Many “adversary lessons learned” evident from the 1990–1991 era were manifested in small-scale contingencies in which the United States was involved during the remainder of the decade, up to and including operations in Kosovo. These lessons included the exploitation of allied communications conducted in clear mode, political sensitivities, and the local geography and environment; the significant payoff of countertargeting efforts; and the importance of contesting air space in some way.

### Kosovo

During the 1999 NATO military campaign in Kosovo, a Study Room was used to conduct an ongoing situational assessment. Again, this served as a mechanism for keeping Laboratory leaders and analysts apprised of unfolding military operation and for enabling collaborative identification of emerging issues. During this effort, key issues and future trends in systems and capabilities, operations and tactics, doctrine and strategy, and force structure and infrastructure were identified.

To the extent that Kosovo was representative of small-scale contingencies, this Study Room captured insights about emerging characteristics of such contingencies, unique military capabilities and concepts required for the effective use of military forces, and lessons learned/implications that could be used in the next Quadrennial Defense Review. To the extent that Kosovo was representative of warfare in the information

age, the Study Room examined the conflict from the perspective that it was the first in which many of the precepts and principles of Network-Centric Warfare could be discerned and which characterized both the observed payoffs and remaining challenges associated with the full implementation and realization of this concept.

## EVOLVING MILITARY REQUIREMENTS

### Joint Warfighting Requirements

One of the most significant military trends evident in the early 1990s was the increased emphasis on “jointness.” This trend, spurred by changes required by the Goldwater–Nichols Act of 1986 and by operational experiences from the Persian Gulf War of 1991, was also a reflection of the changing international environment. With declining defense budgets throughout the international community, partially due to the end of the Cold War and the breakup of the Soviet Union, it was also clear that the United States faced emerging operational, technical, force structure, and fiscal issues which could only be effectively addressed with some type of Joint perspective.

To understand the challenges, opportunities, and long-term implications of this trend for the Laboratory and its sponsors, a Joint Warfighting Requirements Study Room was set up in 1994. This effort initially examined the impact of jointness on military operations, weapon systems, and defense planning and programming. Subsequently, observations regarding the emerging characteristics and implications of jointness were considered in the context of requirements for future capabilities, resulting in recommendations about how the Laboratory and its sponsors should respond to these requirements. Many of the insights were reported to the larger defense community in a previous *Technical Digest* article<sup>1</sup> on the emerging Joint system of systems. Partially as a result of this study and its findings, APL increased the visibility of its efforts in the areas of C<sup>4</sup>ISR (Joint Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) and Joint Warfare Requirements by establishing the Power Projection Systems Department along with JWAD during a 1996 Laboratory reorganization.

### Counterterrorism Activities

A characteristic of the emerging post–Cold War era has been increasing concern about terrorism and the potential vulnerabilities of U.S. populations and infrastructures, both abroad and at home. The bombings of the Khomar Towers, Federal Building in Oklahoma City, and World Trade Center in New York City; the

release of sarin nerve gas in the Tokyo subway; and the loss of an aircraft and many lives over Lockerbie, Scotland, heightened these concerns. In recognition of these emerging threats, the Laboratory initiated a Combating Terrorism Study Room in 1996. Its goal was to help APL leadership assess possible Laboratory roles and involvement in counterterrorism activities. In addition, it addressed the current and emerging threat relative to governmental structures and funding, and legal considerations associated with responses to countering terrorism.

This study concluded that: (1) terrorism was (and is) a growing concern and will continue to pose a significant threat to the country; (2) although significant funding existed for the myriad counterterrorism activities distributed throughout the government and its many agencies, the effectiveness of this funding was somewhat diluted because of a lack of a central focus for counterterrorism activities within federal, state, and local government agencies; and (3) the Laboratory was well positioned to address critical needs in areas such as sensor technology, integrated command systems, information technology, and threat assessment. Partially as a result of this study and its findings, two of APL's new thrust areas identified during the 1998 strategic planning effort were counterproliferation and law enforcement.

## INFORMATION WARFARE

### The Infosphere

Dramatic advances in information technology and the concomitant rise of the Internet have revolutionized the way people, organizations, and states interact, function, and ultimately “behave.” Emerging paradigms associated with the advent of the “information age” have critical relevance both to APL and its sponsors. The Laboratory and JWAD have undertaken a number of initiatives to help sponsors develop a better appreciation for the implications of advances in information, communication, and networking technology for military operations, organizations within the defense community, and American society.

One such initiative was the Infosphere Seminar Project, which began with a seminar for APL leadership in April 1997. Its goals were to identify the implications of Infosphere technology as well as the opportunities it presented, and to identify the implications of Infosphere operations and warfare. Scenarios and Infosphere variants were used to define a range of possibilities in which the impact on military operations and organization structures could be explored. The April seminar was followed by one in May for APL “cyber-specialists.”

The seminars produced several insights, both about military operations and about APL's own functioning.

They underscored the importance of working in an Infosphere environment with an Infosphere-engaged workforce. An effective research and development organization will have Infosphere compatibility in its policies, organization, and environment. Insights from the Infosphere seminars were shared with others in the defense community, through seminars conducted at the Naval War College and the Joint National Test Facility, and via a widely distributed paper entitled *The Navy and the Infosphere* (see the boxed insert). The document

...explores how the Infosphere might evolve, how its development might affect military operations, how the Navy in particular might be affected, and, finally, how defense-related research and development institutions like JHU/APL could be affected.<sup>2</sup>

The Laboratory continued its exploration of information age implications by hosting a series of Cyber

Tech Seminars beginning in 1998. Here leaders from various information enterprises shared their visions of the future in public forums and discussed their implications in small seminars with their peers. Participants in the Cyber Tech Seminars have included world leaders in all aspects of the information revolution: networking, Internet bandwidth and architecture, computer operating systems, high-performance computing, visualization, cyber threats, and information system security. Materials presented at these seminars and synopses of insights from the discussions were made available to APL, the defense community, and the public via the Laboratory's Cyber Tech Seminars Web site (<http://jhuapl.edu/cybertech>).

### Network-Centric Warfare

Although the technology and tenets of the information age were perhaps initially embraced more ardently by commercial organizations, the implications of these changes for military organizations are also quite clear. The adoption and incorporation of information technology and its attendant capabilities in military systems, operations, tactics, doctrine, and organizational changes has become known as Network-Centric Warfare (or Network-Centric Operations).

The concept is easily grasped at a high level, but the details of executing the transition to truly Network-Centric Operations are not so easily described or understood. To help the Laboratory and the Navy better understand these transition issues and implications, JWAD initiated a Network-Centric Warfare Study Room. This effort advanced APL's collaborative approach to problem solving using War and Study Rooms by creating an electronic version of the Study Room (as well as the physical room) with its wallboards and other paraphernalia (see the article by Sinex et al., this issue). The concept has become an integral part of APL's and JWAD's approach to examining emerging, multifaceted, and complex topical areas.

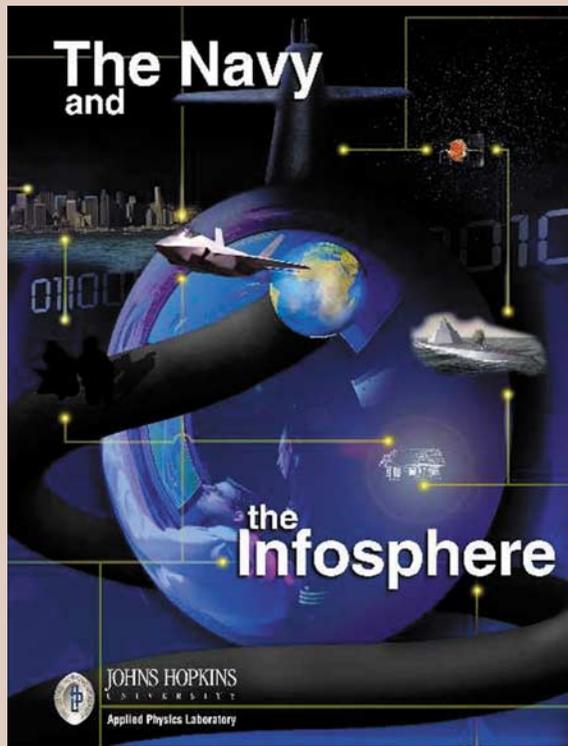
### STRATEGIC PLANNING: TRENDS ASSESSMENT

An important function that JWAD performs for the Laboratory is the identification of trends in the "external environment" that may have important implications for APL and its sponsors. Although JWAD performs this function on a continuing basis, a major review and synthesis of these trends and their implications was completed in support of APL's 1998 strategic planning effort.

Information summarizing trends in these areas was posted on the walls of the External Environment Study Room. Numerous visitors from outside APL— including

#### THE INFOSPHERE

"Infosphere" is shorthand for the fusion of all the world's communications networks, databases, and sources of information into a vast, intertwined, and heterogeneous tapestry of electronic interchange. The global fusion of networks changes the character of each individual network. Networks will no longer serve simply as the medium through which people in different places can communicate, enhancing their *in situ* activities. The global fusion of networks creates a network ecology—literally, a place where people can gather and do business. People will be able to conduct their activities increasingly in the global network ecology, i.e., the Infosphere.



senior military and government leaders, Congressional staff and liaison personnel, officials from The Johns Hopkins University, and senior representatives from organizations similar to APL—were invited to the Study Room to review our findings and provide their perspectives on the future. The research, which was supplemented by discussions with a wide range of people and organizations, developed the context used by other strategic planning activity teams at the Laboratory to ultimately identify new strategic initiatives for APL.

Some of the principal observations and findings from this endeavor were as follows:

- Internationally, it is expected that the United States will remain forward-engaged in an uncertain and turbulent world. Although international defense spending has decreased substantially from Cold War levels, significant threats to U.S. interests persist. The main concern for the future is characterized as the “asymmetric threat.”
- Nationally, it is expected that U.S. defense spending will remain constrained and hard-pressed to meet the needs for readiness, modernization, and force structure. Savings from acquisition reform and infrastructure reduction are intended to provide the additional funds required for modernization.
- In science and technology, there is increasing emphasis on information technology, smart sensors and weapons, complex systems modeling, environmental technology, and health care. In the area of biomedicine and health care, newly emerging infectious diseases, chemical and biological weapons, and genetics are areas of great and increasing interest. Access to health care information and remote treatment will increase worldwide.

## WHAT'S NEXT?

The future has always been an interesting place, perhaps never more so than today as we begin a new millennium. On the one hand, the networked information-dominated world suggested in the *Infosphere* report<sup>2</sup> seems to be a place of incredible promise, both for people and the organizations that make up our society. On the other hand, the U.S. Commission on National Security/21st Century (USCNS/21) has identified several key trends likely to shape our emerging national security environment, including new vulnerabilities created by rapid advances in information and biotechnologies and the evolving global economic infrastructure. Principal among the commission's initial conclusions is the sobering finding that

America will become increasingly vulnerable to hostile attack on our homeland, and our military superiority will not entirely protect us. . . . Americans will likely die on American soil, possibly in large numbers.<sup>3</sup>

The Director of the Central Intelligence Agency, George J. Tenet, also painted a vivid view of this aspect of the future before a 2 February 1999 Senate Armed Services Committee:

In a very real sense, we live at a moment when the past and future are colliding. . . . Today we must deal with terrorists, insurgents, and others who have hundreds of years of history fueling their causes, but chances are they will be using laptop computers, sophisticated encryption, and weaponry their predecessors could not even have imagined.

This “collision” of the past and future can be seen in many areas in addition to these threat concerns. For example, there is an increasing blurring of boundaries between national security and foreign policy, military security and economic security as determinants of national security, national and international organizations and states, discrete states of war and continuous conflict, and weapons of mass destruction and mass disruption. The implications of these colliding perspectives (and the societal, political, governmental, and military transformations likely to occur to accommodate them) constitute clear challenges to our ability to identify future requirements for military capabilities. Indeed, USCNS/21 observes that

The emerging national security environment in the next quarter century will require different military capabilities and other national capabilities (than in the past). . . . The mix and effectiveness of overall American capabilities need to be rethought and adjusted. . . . Discriminating and hard choices will be required.<sup>3</sup>

In an environment where our defense spending (although far more than any other country in the world) is viewed by many as insufficient to provide robust defenses and counters to all of the possible threats to national security, we must, as an analytic community, develop the analytic processes, methodologies, and tools to allow our senior political and military leaders to make critical decisions about future force structures and defense-related investments. To do this, we anticipate that JWAD will continue to undertake initiatives, both in conjunction with directly sponsored work and in anticipation of future sponsor needs, that employ the multistep, iterative Study Room Process described within this article to examine complex issues and create a more coherent understanding of these issues within the defense community.

## REFERENCES

- <sup>1</sup>Manthorpe, W. H. J., “The Emerging Joint System of Systems: A Systems Engineering Challenge and Opportunity for APL,” *Johns Hopkins APL Tech. Dig.* 17(3), 305–313 (1996).
- <sup>2</sup>Vlahos, M., and Pace, D., *The Navy and the Infosphere*, Report JWR-99-002, JHU/APL, Laurel, MD (Mar 1999); also available from the Cyber Tech Seminars Web site at <http://jhuapl.edu/cybertech> (accessed 21 Jan 2000).
- <sup>3</sup>*New World Coming: American Security in the 21st Century*, Phase I Report of the U.S. Commission on National Security/21st Century (15 Sep 1999).

THE AUTHOR



HEIDE E. HEIDPRIEM received a B.S. in electrical engineering from Valparaiso University in 1968, an M.S. in technology of management from The American University in 1976, and an M.S. in technical management from The Johns Hopkins University in 1984. He has extensive experience in systems analysis, test and evaluation, modeling and simulation, seminar-based gaming, requirements analysis, and systems effectiveness assessment. He has held significant management responsibilities in a number of program areas including Fleet Ballistic Missile weapon systems operational analysis; SSBN detectability/vulnerability analysis; and Strike Warfare systems test, evaluation, effectiveness, and survivability analysis. Mr. Heidepriem is currently Supervisor of the Information Analysis Group in the APL Joint Warfare Analysis Department. His e-mail address is [heide.heidepriem@jhuapl.edu](mailto:heide.heidepriem@jhuapl.edu).